DAVE FORREST

BARÁT
vagy
ELLENSÉG?

A totális kontroll forgatókönyve

FOCUS KIADÓ
Budapest, 2005

DAVE FORREST
Friend or Foe? – A Script for the Total Control

Fordította és szakmailag lektorálta: Magyar Tamás,
az Év Biztonságvédelmi Szakembere (2001)

ISBN 963 9468 22 3

Focus Kiadó, 2005
www.sprinterkiado.hu
Felelős kiadó: a Kiadó ügyvezető igazgatója

Nyomtatta és kötötte a Kaposvári Nyomda Kft. – 250666
Felelős vezető: Pogány Zoltán igazgató

TARTALOM

Bevezetés

A XXI. század zűrzavaros világában szinte minden területen az „ember" mint legfejlettebb élőlény kezd háttérbe szorulni, és ezt a helyzetet egyedül saját magának köszönheti. A mérhetetlen tudásvágya – néhol a lustasága – arra ösztönzi, hogy mind fejlettebb és fejlettebb technikát alkosson a maga hasznára – vagy éppen a kárára. Lassan a fejlett technológiák, rendszerek, számítógépek, robotok átveszik a teljes hatalmat és az uralkodást az ember felett.

A fejlődésnek pedig nem lehet gátat szabni, a technika önmagát generálja, félelmetes sebességgel. Ha csupán 50 évet pörgetünk vissza az idő kerekén, láthatjuk, hogy fél évszázadon belül is olyan mértékű változás állt be az életünkben, hogy szinte el sem lehet hinni. Szüleink, dédszüleink csak kapkodják a fejüket, és legyintenek. A mai korosztály már ebbe nőtt bele, ezzel nő fel, számukra ez a természetes. A számítástechnika, a jövőkutatás keresztülkasul behálózza napjainkat, és egyfajta függőséget okoz számunkra.

„Hol a határ?" – tesszük fel a kérdést. A válasz roppant egyszerű. A határt mi, emberek szabhatnánk meg, ha akarnánk. De sajnos ez elképzelhetetlen, mert mindig is lesznek olyanok, akik a „még tökéletesebbre" vágynak, és eközben észre sem veszik, hogy emberi lényük szertefoszlik. Én nem a fejlődés ellen hadakozom, de az idők folyamán már bebizonyosodott, hogy az emberiségnek saját maga is ellensége: úgy, ahogy az általa kifejlesztett technikák és más korszakalkotó vívmányai.

Csupán néhány példa ebből a sorból: atomkor – atombomba – Hirosima; számítógép – internet – intellektuális bűnözés; űrkorszak – űrpajzs – űrháború; mustárgáz – lépfene – Ebola; szintetikus műanyagok – környezetszennyezés – vegyi fegyverek; kard – nyílpuska – interkontinentális rakéta; munkanélküliség – prostitúció – kábítószer; vallási, etnikai, területszerző háborúk – szervezett bűnözés – terrorizmus. Ezek korunk vívmányai! Mind magában rejti a pusztítást és a pusztulást. Erre van szüksége a Föld lakosságának? Nem hiszem!

Csakhogy ezt a folyamatot nem lehet megállítani, legalábbis az ember nem képes erre. Ezért ha tetszik, ha nem, együtt kell élnünk vele, és résen kell lennünk, hogy el ne hatalmasodjon ez a temérdek rossz az életünkben.

Dave Forrest

GLOBALIZÁCIÓmen

Az egységesítés... rossz előjel

A hatalmat uralni vágyó személyek célja egy új pénzügyi, politikai, és életünk minden területére kiterjedő, ellenőrzött világuralmi rendszer kialakítása. Hívhatjuk ezt világdiktatúrának. A globalizációs törekvések már ennek a hatalomnak az előjelei. Nem véletlen, hogy előrelátó, gondolkodó és jóérzésű emberek fellázadnak, és szembeszállnak ezzel a törekvéssel, mert nem akarnak teljesen kiszolgáltatottá válni. Ez a titkos összeesküvés (hegemónia), a hatalomvágy egy világdiktátor vezette egyeduralmi kormány alárendeltjeinek képzeli el a mai kor emberi társadalmát, melyben minden férfi és nő egy önkényuralom rabszolgájává válhat.

A fejlett technikának köszönhetően a világkormány hatékonyabban tudja majd megfigyelni és ellenőrizni alattvalóit, mint bármelyik múltbeli diktatórikus hatalom. George Orwell 1949-ben írt utópisztikus műve, az 1984, most kezd igazán megvalósulni az életünkben. A „Big Brother", a „Nagy Testvér" már nem csak a könyvek lapjain és a televíziók képernyőjén van jelen, hanem az otthonunkban is, és az életünk minden területén.

Könyvem oldalain a tisztelt olvasót egy virtuális gyárlátogatásra hívom, és végigvezetem a „Big Brother Művek" folyosóin. Bepillantást nyerhetnek azokba a titkos laboratóriumokba, ahol az életünket megnehezítő „mestermunkák" kiagyalói dolgoznak, és szövögetik gonosz és aljas terveiket. Ennek a tervnek az a célja, hogy a hatalom vezetői mindent és mindenkit állandó megfigyelés alatt tartsa-

nak, bármikor beavatkozhassanak, és hogy az ő akaratuk érvényesüljön az életünkben. Zárt ajtók mögött egy számítógépesített rabszolgarendszert terveznek, melyet folyamatosan tesztelnek különböző országok mit sem sejtő állampolgárain, és vezetik be világszerte. Ez a terv számos technikai, gazdasági, politikai összetevőből áll, és háttérinformáció nélkül nehéz felfedezni.

Könyvemből megismerhetik az emberek megfigyelésére, nyomon követésére, az információk megszerzésére használt eljárásokat, taktikákat, az ehhez szükséges eszközöket, az azonosítás módszereit, majd a totális ellenőrzés és irányítás emberi elmét felülmúló tervét.

OMEGA-KÓDex

A Végső Terv forgatókönyve

A terven gyanútlan emberek dolgoznak, olyanok, akik a szakmájukban elismertek, komoly eredményeket értek el, Nobel-díjakat kaptak, egész kutatólaboratóriumok állnak a szolgálatukban; alkalmazottak százai, ezrei lesik minden parancsukat és óhajukat. Ezek az emberek azért tanultak és fejlesztették tudásukat, hogy aztán rabszolgaként, földi alamizsnákért az emberiség leigázásában vegyenek részt. Olyan tudás birtokában vannak, hogy ebből a rendszerből nincs lehetőségük élve kiszállni.

Megbízóik kényesen ügyelnek arra, hogy a titkos terv részletei ne szivárogjanak ki a külvilág felé, mert az felboríthatná az elképzeléseiket. Aki pedig az útjukban áll, azt könyörtelenül félreállítják. Minden alantas módszert igénybe vesznek, hogy a nekik dolgozó személyeknek ne legyen kedvük „kitálalni" az információkat. Az a félelmetes, hogy aki számukra fontos, azt a tudta és akarata nélkül szervezik be, azért, hogy még választási lehetősége se legyen.

A fontos személyről minden létező információt összegyűjtenek, majd kielemzik, és megkeresik a gyenge pontját. Aki állandó pénzzavarral küzd, annak komoly fizetést; aki egy „lyukban" lakik, annak szép lakást; aki gyalog jár, annak vadonatúj autót; aki hírnévre, sikerre vágyik, annak azt ígérnek. Aki utazni szeretne, annak világ körüli utat; akinek nincsen munkahelye, annak hosszú távú álláslehetőséget ajánlanak fel – egy aláírásért, amellyel egy életre eladja magát egy olyan rendszernek, amely csak eszköznek tekinti a személyét, és ha már feleslegessé vált, egyszerűen félretolja.

Ha a személy nem korrumpálható, akkor más módszerhez folyamodnak. Szintén a gyenge pontjait, a jellemhibáit használják ki. Ha férfi az illető, akkor elcsábíttatják egy már beszervezett nővel, hogy aztán különböző (test)helyzetekben kompromittáló felvételeket készítsenek róla (természetesen titokban). Utána meg jön a zsarolás a családdal, médiával, karrierrel. De az sem ritka módszer, hogy a szakszolgálatok például egy elkövetett bűncselekményét (baklövését) semmisnek minősítik, és cserébe „csak" egy kis szívességet kérnek tőle.

A legdrasztikusabb, amikor a család, feleség, gyerek élete van veszélyben. A családjukat szerető, és más módon nem kompromittálható személyek ellenállását azzal lehet megtörni, hogy beígérik a férj vagy a feleség, a gyerekek elrablását vagy meggyilkolását. Mielőtt megkeresnék a célszemélyt, már tudják róla, hogy melyik lehetőséget használják fel vele szemben. Ezek a dolgok nem csak a filmekben vannak, így nem is fikciók. Ezt a módszert használják az ügynök- és hírszerző szolgálatok is, (amikor egy lényeges információt akarnak megszerezni), olyan személyek, akikben nincsen gátlásosság, emberség, együttérzés, és egyáltalán nincsen lelkiismeret-furdalásuk. Egyszerűen sarokba szorítják az embert, és nagyon kevesen tudnak ellenszegülni egy ilyen erős nyomásnak. Egy dolog vezérli őket: uralkodni mások felett, hogy ők lehessenek élet és halál urai. Egyet viszont elfelejtenek: ez a feladat NEM NEKIK ADATOTT MEG! Ezért mindaz, amit elkövetnek embertársaik ellen, az aljas, gonosz cselekedet, és nem marad válasz nélkül. Tetteikkel a saját sírjukat ássák.

A rendszert a világ leghatalmasabb és legbefolyásosabb csúcstechnikai vállalatai, bankjai, hírszerző szolgálatai és rendfenntartó alakulatai fejlesztik, amelyek minél hatékonyabb és fejlettebb emberellenőrzési eszközök feltalálásán dolgoznak: lehallgatóberendezéseken, mikrochipeken, kémrendszereken, megfigyelőrendszereken, a mesterséges intelligencia és a „virtuális valóság" eszközein. Ennek érdekében mérnökök, programozók és tudósok millióit alkalmazzák. Ezért keresik annyira és fizetik meg olyan jól a számítástechnikai szakembereket, a villamosmérnököket, fizikusokat, pénzügyi szakembereket. Gyászos kimenetelű terveken dolgoztatják őket, de ők nincsenek ennek tudatában, mivel időbe telik, míg megszokják az új környezetüket, és felfogják, mi is folyik a színfalak mögött. Általában részfeladatokat kapnak, és a „fejlesztőtársaikat", akik a projekt más összetevőin dolgoznak, nem is ismerik.

A Terv kiagyalói képesek még a legőszintébb, gyanútlan balekokkal és beépített emberekkel is elvégeztetni piszkos munkájukat. Felmérhetetlen károkat okozhatnak az életünkben a világ vezető csúcstechnikai intézményeinek és laboratóriumainak folyosóit róvó briliáns elméjű, de lelkileg tudatlan emberek által a mi ellenőrzésünkre kifejlesztett termékek.

A számítógépesített globális ellenőrzési rendszer megköveteli minden egyes ember folyamatos azonosítását, bárhol is él a Földön. Nevünk, címünk, születési időnk és helyünk már szerepel gépjárművezetői engedélyünkön, egészségügyi igazolványunkon, útlevelünkön, személyi igazolványunkon. Ezekre és a hasonló plasztikkártyára egy-egy egyedi szám van nyomtatva vagy dombornyomva. Bebillentyűzve vagy kártyaolvasóval beolvasva ezeket a számokat egy számítógépbe, az adatbázisokban rólunk tárolt információ elolvasható. A kártyákon levő mágnescsíkok is sok információt tartalmaznak, az új, parányi mikrochipek pedig több ezer oldalt is tárolhatnak.

A „pozitív", azaz egyértelmű azonosításhoz a következő, személyenként eltérő, egyedi élettani vagy viselkedési jellemzőket használják: aláírás, arckép, ujjlenyomat, talplenyomat, hangtónus, DNS-genotípus, fehérvérsejt-antigén, kézgeometria, az arc vagy a csukló ereinek hálózata, a szem retinájának vagy íriszének mintázata. Ezeket a jellemzőket bonyolult műszerek és különféle érzékelők segítségével lemérik, majd digitalizálják és számítógépes adatbázisokban tárolják, a későbbi összehasonlítás céljából. A személyek azonossága leellenőrizhető, digitálisan lemérve a kiválasztott biológiai jellemzőt, és összehasonlítva az adatbázisban tárolt referenciamintával. Minden rögzített érték egy (egyedi) személyi számhoz van csatolva, így bármelyik összetevőt vizsgálják, bárhol a világon, mindig ugyanaz a személy azonosítható be általa.

BIOMETRIAdalom

Az emberi azonosítás eszköze

Ezt a technológiát biometriának nevezik, és már az egész világon alkalmazzák bankokban, pénzkiadó automatáknál, repülőtereken, hatóságoknál. A kétdimenziós arcfelismerő rendszerek videokamerák segítségével hasonlítják össze egy személy arcát egy tárolt képpel. Az arcról készített képet digitálissá alakítják, kielemzik, majd összehasonlítják egy előzőleg készített és számítógépen vagy azonosító kártyán tárolt változattal. Ezt a módszert számítógépesített biztonsági és beléptetési rendszereknél is használják már.

A háromdimenziós arcfelismerési rendszer egyelőre biztonsági rendszereket szolgál, ám hamarosan mindennapi életünk tartozéka lehet. Feltéve, ha sikerül olyan tökéletessé fejleszteni, hogy nem lehet megtéveszteni különböző technikákkal. Elég egy maszkmester által készített profi szakáll, egy fogorvosi tampon a felső fogíny és arccsont közé, és máris egy, a rendszer számára azonosíthatatlan személy képe jelenik meg a képernyőn.

Tökéletlensége ellenére az arcfelismerő technológiát mégis számos helyen alkalmazzák. A rendőrség törvényszéki áttörésnek tartja, és az új, üzembiztos, háromdimenziós változat a pénztáraknál és a munkahelyeken mindennapos rutinná válhat. Erre a területre kiválóan alkalmas, mivel itt pont az a cél, hogy az idegeneket, a jogosulatlan személyeket kiszűrje. Napjainkra a sci-fi védett területe, a biometrikus arcfelismerő rendszer már valóság. Az azonosító kártyák által felvetett viták ellenére ez a technológia is a mindennapi életünk egyik alapeleme lett.

Már most is van jó néhány szervezet, mely alkalmazottainak a rendszerekhez történő teljes hozzáférést az arckép beszkennelésével adja meg. Ez a rendszer még biztonságosabbá tehető, ha hőkamerát is párosítanak hozzá, amely az arc bizonyos (jellegzetes) pontjain keletkező, és egyedre jellemző hőképeket is rögzíti. Ahogy az egyes cégek egyre nagyobb hangsúlyt fektetnek a biztonsági eljárásokra, a beszkennelt arcok egyre inkább mindennapossá válnak. Az új technológia, mely tökéletes, háromdimenziós módon teszi ezt meg, forradalmasíthatja ezt a trendet.

A háromdimenziós szoftvert kifejlesztő cég a programjukat olyan precíznek ítéli meg, hogy az akár még az egypetéjű ikrek között is különbséget tud tenni néhány másodperc alatt. A letapogatógép infravörös fénnyel az emberi arcról 16 felvételt készít, és mint egy virtuális hálót, mátrixszerűen összemossa egyetlen sablonná, amiből kiszámítja az arc jellegzetességeinek méreteit. A kép elméletileg azonnal ellenőrizhető egy adatbázis segítségével, így vezérelhető az épület egyes részeihez vagy a pénztárgépekhez való hozzáférés.

A már létező biometrikus arcteszteket – melyek egyelőre kétdimenziósak – jelentősen befolyásolják a megvilágításban és az arckifejezésekben, a karakterisztikus pontokban bekövetkező változások. Az angol kormány biometrikus próbálkozásai az útlevelek és személyi azonosító kártyák esetén 10%-os hibaarányt mutattak a kétdimenziós arcfelismerésnél. Az Aurora szoftvere ellenben kiküszöböli ezeket a hibákat. Hugh Carr-Archer alapító szerint a program százszázalékosan működik, melyeket az elvégzett tesztek is igazolták. A program működésekor a gyanúsított arcképét beszkennelik – mint a CCTV (zártkörű tévélánc) technikával készített helyszíni képek, vagy a szemtanú által leírt arcképek. Ez elkészíti az arc kétdimenziós térképét, mely

már jelöli annak jellegzetességeit, a szemek közötti távolságot. Ezt követően egy számítógép algoritmusok segítségével összehasonlítja az arc adatait az adatbázisban tárolt arcok adataival. Másodperceken belül kidobja a megfelelő egyezést, az egész úgy működik, mint egy webböngésző.

A fenti elven működő arcfelismerő biztonsági rendszert fejlesztettek ki nemrég számítógépek számára. A szoftver a bekapcsolt számítógép használatát akadályozza meg a képernyő lezárásával. A biztonsági rendszer csak akkor old fel, ha megjelenik a jogosult felhasználó arca a monitor előtt. A monitorba épített miniatűr kamera a felhasználón kívül egyúttal a környező területet is figyeli, és minden oda belépő személyt megörökít annak tudtával vagy tudta nélkül, ha akarja, ha nem. A képek egy távfelügyelő rendszerhez is továbbíthatóak. A gyártó és forgalmazó cég ezt nem nevezi kémkedésnek, hanem csupán olyan rendszernek, amely őrzi a számítógépet és a környezetét... Jó ötlet! De kinek?

Ki a tényleges felhasználója az ilyen és ehhez hasonló, mindent látó, halló és továbbító rendszereknek? Miért szorgalmazzák ezek használatát? Ráadásul külön nem is kell érte már fizetni, mert eleve beintegrálják a konfigurációkba. Nem hagyják meg azt a lehetőséget sem a számunkra, hogy kérjük-e ezt az opciót vagy nem. A legegyszerűbben úgy védekezhetünk ez ellen, hogy egy szép hímzett terítővel letakarjuk a méregdrága LCD monitorunkat. A terítőre hímeztessük rá azt, hogy „The Big Brother is Watching You".

Az American Biometric Company terméke, a BioMouse nevű ujjlenyomat-leolvasó jó példa a csúcstechnikájú daktiloszkópiára. Számítógéphez kötve a BioMouse a felhasználót ujjlenyomata alapján azonosítja, és az eredménytől függően engedélyezi vagy megtiltja neki a számítógép használatát, azaz a „feledékenyebbek" kedvéért felváltja a

jelszót. Ezt a technológiát számos területen használják már. Viszont ha az egér le bírja olvasni a felhasználó ujjlenyomatát, akkor a működéséhez szükséges azonosító szoftver nem csak a raktározására, azonosítására képes, hanem az elküldésére is. Így az ujjlenyomataink védtelenül kószálhatnak a világhálón anélkül, hogy tudnánk róla, amíg egy ügyes szakember fel nem használja a maga hasznára.

Például a jogtalanul megszerzett ujjlenyomatom segítségével reprodukálnak egy teljesen egyező műujjat, elég egy is belőle (bármelyik ujj), s azt egy bűncselekmény (például egy gyilkosság) elkövetésekor a bűnöző felhúzza az ujjára, és tudatosan hagy nyomot az elkövetés helyszínén. A helyszínelők megtalálják a nyomokat, és miután beazonosították, kopognak mit sem sejtő, vétlen személyem otthonának ajtaján, és már kattan is a bilincs a csuklómon. Mondhatok én akármit, ők a rögzített nyomoknak hisznek. Ugye, milyen morbid történet? De nem csak morbid, nagyon veszélyes is ez a szituáció!

„Megnyugtatásul" közlöm: ennek a csapdának van kitéve a többi egyedi azonosító jegyünk is. A mai, modern technológiákkal mindent tökéletesen le tudnak másolni, például olyan kontaktlencsét is lehet már gyártani, ami hibátlan másolata az eredeti mintázatnak, és behelyezve a szemgolyóra már be is csapták az íriszazonosítót. A sci-fi filmekben láthatjuk ezeket a trükköket, mégsem fogják fel sokan, hogy ez már a valóság része. A forgatókönyvírók az életből merítik az ötleteiket, nem ők fejlesztik ki a szupertitkos eszközöket. Én kizárólag ezért nézem meg az ilyen jellegű filmeket. Nem a bugyuta sztori érdekel, hanem a technológiák bemutatása. A „007-es ügynök"-történetek vagy a Mission Impossible jó példák erre, melyekben olyan szupertechnikákat vonultatnak fel, hogy csak pislogunk a csodálkozástól.

Egyes autógyártó cégek már kulcsokat sem használnak. RFID (rádiófrekvenciás) chipkártyával és a tulajdonos ujjának együttes használatával engedélyezik a motor beindítását. Ám az azonosító, úgynevezett „bio" szenzorokat nem lehet becsapni, mivel egyazon időben több olyan vizsgálatot elvégeznek az ujj bőrén, amelyet csak az élő szövetekkel lehetséges, és ezzel kizárják azt is, hogy valaki egy látszatra hasonló műujjal próbálkozzon, vagy ami szintén előfordult már, például banki széf kinyitásánál, hogy a tulajdonos levágott ujját akarták felhasználni a pénz megszerzéséhez... Az élettelen ujj bőre nem produkálta azokat a paramétereket, amelyekre szükség lett volna. Ilyenek például a bőr ph-értéke, nyirkossága, elektromos töltése (ellenállása), az ujjbegyek hajszálereinek kapilláris mozgása.

A rendszerek úgy vannak beállítva, hogy amikor ilyen eltérést észlelnek, látszatra megkezdik a műveletek végrehajtását, de közben sürgősségi riasztást generálnak a rendszer központja felé, ahonnan megindíthatják a biztonsági ellenintézkedést. Egy további lehetőség, hogy a kényszerített tulajdonos nem azt az ujját teszi a leolvasó szenzorra, amelyik a pozitív azonosításhoz kell, hanem az úgynevezett riasztó ujjat (előre betáplált másik ujj), amelynél a rendszer egyértelműen riasztást generál, és beindítja az ellenintézkedést.

A külső szemlélők (rossz fiúk) semmit nem vesznek észre ebből a műveletből. A fenti példákból is látható, hogy az egyre bonyolultabb rendszerek egyre jobban megkívánják a használóik egyedi azonosíthatóságát. Ezzel is még jobban hozzájuk kötve a tulajdonosukat, ami azt jelenti, hogy sokkal egyszerűbb a személyhez kötni valamilyen cselekménysort. A genetikai tulajdonságok hamisíthatatlan, természetes pecsétek, melyekkel egyediségünket igazolhatjuk. De vajon

a Teremtés és az egyedfejlődés során azért kaptuk e tulajdonságainkat, hogy aztán pont ezeket fordítsák ellenünk?

A kézfejen a vénák rajzolata össze nem téveszthető ujjlenyomatként működhet, vagyis alkalmas a megbízható személyazonosításra. Az Ázsiában kifejlesztett módszer infravörös szkenner segítségével felismeri a vénák egyénre jellemző mintázatát. A szem íriszének, azaz szivárványhártyájának leolvasása és kielemzése még egy másodpercet sem vesz igénybe. A személy íriszének videokamerával felvett képét digitális formában adatbázisban tárolják. Később a személy felismerhető írisze alapján, ha a kamera felé néz. A jövő pénzkiadó bankautomatáin (ATM-ek) rejtett videokamerákat használó íriszazonosító berendezések lehetnek. Ezek összehasonlítják majd az ügyfél íriszének képét a bankkártyáján vagy a bank adatbázisában tárolt referenciaképpel, hogy megállapíthassák személyazonosságát. Az eredménytől függően megengedik vagy megtiltják a kívánt tranzakció elvégzését.

Régebben a rendőrség mintát vett a bűnözők ujjlenyomatáról, hogy nyomon követhesse őket, amint különféle tárgyakhoz érnek. Ezt a módszert megalázónak tekintették, és az is volt. Most meg minden technikai újdonságnak tapsolnak a szakemberek. A mostani eljárások egyre kifinomultabbak, mi pedig mindnyájan „rabszolgákká" válunk uraink globális ültetvényén, mert kitaláltak egy olyan diktatúrát, amelyben mindannyiunkat egy központi számítógépes nyomon követő rendszerhez kapcsolnak, mintha mind „bűnözők" volnánk, jegyzékbe kellene venni és nyomon követni bennünket. Ideje lenne felébredni a Csipkerózsika-álomból, mert így azt tehetnek velünk, amit csak akarnak...

GENETIKAlmárok

Génkereskedők

A világon már több országban léteznek genetikai adatbankok, amelyek több millió ember vér-, nyál- és szagmintáját tárolják. A minták újszülöttektől, valamint a hadsereg újoncaitól, bűnözőktől stb. vett vérből, nyálból és testszagokból származnak. Ezeknek a mintavételeknek a célját nem verik nagydobra, úgy tűnhet a szemlélőnek vagy az alanynak, mint egy rutineljárás. Ki merne szólni egy kórházban a munkáját végző nővérnek, amikor a tűt beleszúrja a bőre alá, vagy a szájába nyomja a nyálmintavevő „nyalókát"? Miután levették a mintát, ki tudja, hogy milyen vizsgálatokra használják fel azokat, egyáltalán hova kerülnek?

Egyes országokban a „hatóságok nyilvántartást vezethetnek a gyanúsítottak DNS-profiljáról", amihez nyál- és hajmintát vesznek tőlük. Rendeletben írják elő a bűnügyi nyilvántartások számára ujj- és tenyérlenyomatok, fényképek készítésének a részletes szabályait is, ami jogbiztonsági szempontból komoly előrelépés. Viszont ez most már a szemtanúkra is kiterjed. A szemtanúktól, sőt a sértettől és annak családtagjaitól is vehetnek le azonosításra alkalmas ujj- és tenyérlenyomatot arra hivatkozva, hogy a bűncselekmény helyszínén rögzített nyomok közül így könnyebben meg tudják találni az elkövető személyét. A vétlen személyektől levett nyomokat az ügy lezárása után nem törlik az adatbázisból: bekerülnek abba a bizonyos mátrixrendszerbe, így azok örökre benn maradnak, és bármikor elővehetők, mindig kéznél vannak! Ezek a genetikai

„ujjlenyomatok" veszélyeztetik az emberek magánélethez való jogát.

Sikernek és szenzációnak könyvelik el az állatok klónozását. De mi lesz, amikor embereket fognak klónozni? Genetikailag beavatkoztak már eddig is a teremtésbe a tudósok, de az emberi faj mesterséges másolása beláthatatlan következményekkel járhat. A lombikbébiprogramok már ennek az eseménynek az előjelei (szerintem tudatos próbálkozásai). A gyermek után vágyakozó szülők már most is meghatározhatják leendő gyermekük összes paraméterét, a lélek és a szellem kivételével. Viszont ez a két tulajdonság teszi az embert emberré. Ezt soha nem tudják másolni, minden más tulajdonságot igen. Ebben van a legnagyobb veszély, mert nem tudhatjuk, hogy mivé válhatnak a fejlődésük során az ember által alkotott „mesterséges" lények – gondoljunk csak Frankensteinre!

Mivel a kísérletek még olyan stádiumban vannak, hogy nem áll rendelkezésre egy emberéletnyi tapasztalat, így a tudósok is csak találgatni tudnak a jövővel kapcsolatban. Isten is megformázta az ember testét, de az élet akkor költözött belé, amikor a Teremtője belelehelte a lelket. A növények és az állatok mesterséges szaporítása már nem újdonság. Emberi szemmel nehéz lenne megkülönböztetni az egyformának tűnő csirkéket, libákat és más állatokat, a növényekről nem is beszélve. Mesterséges szelekcióval a tökéletes egyedek létrehozására törekednek. A sérült, degenerált géneket lokalizálják és kimetszik a fejlődési láncból anélkül, hogy kárt tennének az egyed fejlődésében. Ez fantasztikus nagy lépés a tudomány részéről, de így nem csak a beteg géneket tudják manipulálni, az egészségeseket is meg tudják változtatni, olyanná, amilyenné akarják.

A géntérkép a rendelkezésre áll, és a génsebészek a zöld lámpát várják, hogy megalkossák az első klónozott embert. Vagy már él és virul valamelyik szigorúan titkos, föld alatti szuperlaboratórium falai között? Miért is ne? Hiszen évtizedekig arról sem tudtunk, hogy Amerikában egy titkos bázison ufonautákat rejtegetnek, és különböző kísérleteket végeznek rajtuk. Hát ez az, amiről beszélek! Mint már írtam, az emberiség nagyon kis csoportjának adatik meg, hogy beleszólása legyen a történésekbe. (Nem árt, ha önök is tisztában vannak vele, hogy kik azok a személyek, akik a top 100-as listán szerepelnek, ahol még mindig Bill Gates van az első helyen!) Ők ezt tudják magukról, és élnek is a hatalmukkal. Mi meg kénytelenek vagyunk elfogadni azt, amit elénk tálalnak. De „bevenni" és „megenni" nem kötelező mindent!

KIBERNETIKAlandorok

Emberi robotok

A génsebészet és a robotechnika közös végtermékeként rövidesen megszületnek a „human robotok", a ránk hasonlító hardverek. Olyan lények, amelyek nem gondolkodnak, és csak parancsvégrehajtásra vannak beprogramozva. Mivel nem vegetatív élőlények, így nincsen szükségük táplálékra, pihenésre, képesek folyamatos feladatvégzésre. Mikrochipek és speciális anyagok alkotják a testüket.

Szívük helyén tölthető akkumulátor biztosítja a szükséges energiát. Szemgolyójukba speciális, többfunkciós, miniatűr kamerákat építenek be, melyek érzékelik a környezeti és fényviszonyokat; hallójárataikba mindent halló mikrofonokat helyeznek el. A műholdak segítségével bárhonnan irányíthatóak. Külső borításként az emberi bőrrel azonos tulajdonságú és a sebészetben már használatos anyagokat használnak fel.

A Terminátor és az ehhez hasonló filmek ezt a korszakot vetítették elénk annak idején, most meg már benne élünk. A filmek segítségével fölkészítettek bennünket a fogadásukra, és meg akartak minket kímélni a sokkhatásoktól. Ez sikerült is, mert már természetes számunkra, hogy vannak gondolkodó robotok, amelyek kommunikálnak velünk és egymással, felismerik a környezetüket, és váratlan eseményekre is reagálnak valamilyen szinten.

Az automatizálás alapja a robotechnika, melynek veszélyes következménye, hogy fölöslegessé válik az emberi erő, ami növelni fogja a munkanélküliséget. A multinacionális cégeknek megéri a méregdrága robotok üzemeltetése, mert a robot nem fárad el, nem éhes, nem beszél vissza és nem kér fizetést, azt csinálja, amire be van programozva, vagyis ő az ideális munkaerő.

Életünk minden területén megjelentek már ezek a „kényelmi eszközök", melyek identitásunkat, sőt emberi mivoltunkat is veszélyeztetik. A tökéletes másolatok kora itt van a küszöbünkön. Jogosan mesélhetjük az unokáinknak a Teremtés történetét, amikor is Isten a saját képmására teremtette az embert, és az ember a maga képmására megteremtette a robotot! Annyival könnyebb az én helyzetem Asimovnál, Verne Gyulánál és Orwellnél, hogy nekem nem víziókat kell megálmodnom a könyvem megírásához, hanem a technika jelenlegi állapotával kell tisztában lennem.

INFORMATIKAlózok

A számítástechnika vámszedői

A globális ültetvényt irányító rendszer („az irtózatos sebességgel fejlődő technikának köszönhetően") teljesen számítógépesített. A sebességet úgy lehetne meghatározni a legegyszerűbben, hogy az ebben a pillanatban az áruházak polcaira kerülő technikai újdonság a kikerülésével egy időben már el is avult... Hihetetlennek hangzik, de ez abból adódik, hogy a különböző cégek fejlesztései nem azonos időben indultak el, és ezért valamelyik mindig előrébb jár egy lépéssel. Az átlagember pedig ki van téve egyfajta nyomásnak, amikor döntenie kell, hogy melyik eszközt vásárolja meg. Ezért lehet „fillérekért" manapság hozzájutni a modern ketyerékhez, mert a cégek a számukra új, de a piac számára már elavult termékeiktől, ha kis haszonnal is, de meg akarnak szabadulni, hogy legalább a fejlesztés költségeit visszakaphassák. Nem irigylem a gyártókat, mert ha nem tudnak újat és még újabbat produkálni, lehúzhatják a rolót a cégüknél.

Minden ország hatalmas összegeket költ a nemzeti számítástechnikai fejlesztésekre. Az állampolgároknak azt mondják, hogy mindezt az ő biztonságuk, védelmük és magas életszínvonaluk érdekében teszik, vagy azt hozzák fel mentségként, hogy nem lehet technikailag lemaradni a globális gazdaságban. Ez sajnos igaz, de megkérdeznek bennünket, hogy akarjuk-e ezeket? Hát persze, hogy NEM! Ez a rendszer a beleegyezésünk nélkül épül, eldöntötték helyettünk, és folyamatosan bővítik.

A világon levő számítógépek száma exponenciálisan

növekszik, a számítógépes hálózatok pedig már az egész Földet körülölelik. A végső cél az, hogy minden ember össze legyen kötve egy számítógéppel, internetes kapcsolattal és mobiltelefonnal, amelyek online kapcsolatban vannak a „Központi Aggyal". Az eszközöket gyártó cégek sem véletlenül adják már szinte ingyen (szuperakciók, vissza nem térő lehetőségek keretein belül) a mindentudó telefonjaikat, a „kedvezményes" internet-elérhetőségeket, „államilag támogatott" számítógépeket. Csak így tudják minden lakásba, közintézménybe és a gyanútlan emberek életébe betenni a lábukat, és ha már bent vannak, ott is akarnak maradni (hűségnyilatkozatot íratnak alá).

Ráadásul ahhoz, hogy valaki „kedvező áron" bekerülhessen a rendszerbe, a vásárlásnál vagy a telepítésnél minden adatára szükség van, így rögtön a környezettanulmány is elkészülhet róla, és ez fel sem tűnik a gyanútlan vásárlónak, mert a szeme könnybe lábad az örömtől, hogy otthonába viheti a régen áhított konfigurációt vagy modemet. Alig várja már, hogy lenyomhassa az enter billentyűt és felkapcsolódhasson az internet-mátrixra, hogy aztán kinyissa az ajtót az életébe ismeretlenül betolakodóknak. Az emberek megbűvölten ülnek a mozivászon előtt, amikor a Mátrix című filmet vetítik. Bele sem gondolnak abba, hogy ez a jelen valóságot vetíti a szemük elé. Neo és társai itt vannak már közöttünk, csak más néven. Nézzenek jobban körül! Most biztosan önök közül sokan elmosolyodnak. Nekem viszont, aki naponta szembesülök ezekkel az általam leírt dolgokkal, nincsen kedvem mosolyogni.

Manapság már azt tekintik furcsa embernek, akinek nincsen telefonja, számítógépe, tévéje, nem csatlakozik az internetre, nem használ bankkártyát, holott a jelek azt mutatják, hogy ő a bölcsebb. Az adatbázisok száma és a

bennük tárolt információ mennyisége is vészesen nő. Mindez köztudott. Ellenben kevésbé ismert, hogy ezek az adatbázisok országosan és nemzetközileg is kapcsolódnak már egymáshoz. Bankok, cégek és állami szervek osztoznak az állampolgárok legfontosabb adatain, a tulajdonosuk beleegyezése nélkül. Az adóhivatal, szociális és egészségügyi intézmények, biztosítótársaságok, bankok, viszonteladók, közlekedésrendészet és még ki tudja, kicsodák, mind elektronikus kapcsolatban állnak egymással. Ez a Mátrix pedig napról napra növekszik.

A műholdak jóvoltából a Földünkön nincsen már olyan hely, ahonnan ne lehetne kommunikálni, az Égi Szemek mindent és mindenkit látnak, mi viszont, egyszerű halandók azt sem tudjuk, hogy azok hol vannak pontosan. Éjszaka, amikor felnézünk a tiszta, csillagos égboltra, és gyorsan mozgó fénypontra leszünk figyelmesek, legyintünk, és azt mondjuk: ufó, pedig az valószínűleg egy kémműhold a sok százból vagy ezerből, és lehet, hogy pont mirólunk küld információkat valahová az ismeretlenbe.

A számítástechnika fejlődésének robbanásából, valamint a központi szerverek és adatbázisok társadalombiztosítási számon keresztüli összekapcsolásából jött létre egy olyan helyi, regionális, országos, kontinentális és az egész világra kiterjedő számítógépes hálózat, amelynek segítségével az állami irányító és védelmi szervek gyakorlatilag azonnal hozzájuthatnak a saját vagy hozzátartozóink bármely, vagy akár az összes adatához, beleértve egész életünket, pénzügyeinket és cselekedeteinket, gyakorlatilag a bölcsőnktől a sírunkig.

Az élet szinte minden területének számítógépesítése (legfőképpen a pénzügyeké) és az adatbázisok összekapcsolása lehetővé teszi egy viszonylag kis csoportnak, hogy átvegye a hatalmat az egész világ fölött, és véget vessen az emberek Istentől kapott szabadságának. Számomra ez a felismerés hátborzongató, sőt horrorisztikusnak tűnik, és hogy ez már a jelenünkhöz tartozik, egyenesen aggodalommal fog el.

VONALKÓDiktatúra

Vonalkód-egyeduralom

Mindenáron meg akarnak bennünket jelölni egyedi azonosítókkal, ezért először a környezetünkben található összes tárgyat megjelölik, hogy aztán erre hivatkozva, „a tökéletes rendszer igénye szerint" rásüthessenek minden emberre egy egyedi számot.

A vonalkód világszerte használt azonosítási eszköz, amellyel bármely személyről, helyről vagy dologról adatot lehet gyűjteni, de elsősorban tárgyak, különféle árucikkek, dokumentumok, plasztikkártyák nyomon követésére használják. Vonalkódot nyomtatnak a termékek széles skálájára, enélkül már nem is kerülhet forgalomba semmilyen áru.

A vonalkód változó szélességű, egymással párhuzamos sötét sávokból és helyközökből áll. Egy adott termék azonosítási számát jelképezi, és megegyezik az alatta levő nyomtatott számsorral. Egy hagyományos vonalkódban 30 fekete függőleges vonal van. A vonalkód szélein és közepén két-két hosszabb vonal található, amelyeket „őrvonalaknak" neveznek, és amelyek vonatkozási pontok a számítógépes leolvasónak. Ezek között van egy 12 számjegyű kód két, 6 számjegyből álló fele. Minden számjegy 2 vonal és 2 helyköz kombinációjából áll.

A legtöbb vonalkód a termék származási országát, a gyártó céget és az adott terméket azonosítja. Kimért áruk, például zöldségek esetén a szupermarketekben a vonalkód a termék típusát, azonosítóját és súlyát jelöli. Az újságokon és könyveken levő vonalkódokban benne van ezen

áruk nemzetközileg egységes ISSN-, illetve ISBN-száma. A pénztárgép a termék vonalkódjának leolvasása után kikeresi a hozzá tartozó árat a bolt számítógéprendszeréből.

A kereskedelmet felügyelő szervezetek ráerőszakolták a kereskedőkre a leolvasó rendszereket. Nem árt tudni, hogy ahol online kapcsolat van kiépítve a rendelésekhez és a terméknyilvántartásokhoz, ott a rendszer oda-vissza működik, tehát bármikor, bárki (magán- vagy állami szervek), bárhonnan a tulajdonosok tudta nélkül beletekinthet a készletnyilvántartásba, leltárba, pénztárkönyvekbe és a könyvelésbe.

Az adóhatóságoknak a mai modern pénztárgépek segítségével könnyű dolguk van. Ellenőrzéskor a gépek memóriájában rögzített adatok mindent elárulnak, másodpercre készen. A hitelesített gépeket pedig nem lehet manipulálni, így lettek kitalálva. Elég egy próbavásárláskor be nem ütött összeg, és máris röpködnek a bírságok. Semmiség egy termék árát megváltoztatni, mert elégséges csupán egyszer átírni a számítógépes adatbázisban. Ha külső szabotázs jellegű támadás ér egy számítógépesített kereskedelmi láncot, a teljes rendszer összedőlhet egy gombnyomásra, komoly károkat okozva ezzel a tulajdonosainak. A diktatúra tervében szerepel, hogy a Földön mindenkinek egy 18 számjegyből álló egyedi azonosítási kódot osszanak ki, mely 3 különálló 6 számjegyű sorozatból állna.

Az Ohióban (USA) élő Richard Thomas a „COMPUTER" szó tanulmányozása közben rájött egy összefüggésre: az ABC minden betűjét behelyettesítette egy hattal osztható számmal, és a hatossal kezdte: A/6, B/12, C/18, D/24, E/30, F/36, G/42, H/48, I/54, J/60, K/66, L/72, M/78, N/84, O/90, P/96, Q/102, R/108, S/114, T/120, U/126, V/132, W/138, X/144, Y/150, Z/156. Ha most összeadják a Computer szó

betűihez tartozó számokat, különös számot kapnak. De ez már számmisztika, és semmilyen valós alappal nem rendelkezik. Ezzel a számítással még nagyon sok nevet és fogalmat lehet összekapcsolni a végeredményben szereplő háromjegyű számmal. Ezt csak érdekességképpen mutattam be önöknek. De mi van, hogyha ez az állítás is igaz? Gondoljuk át, hogy milyen függőség alakult ki ember és komputer között napjainkra!

A világon levő minden termék és pénz fölötti ellenőrzés megszerzéséhez bevezették az ISO-9000 minősítési rendszert (és továbbfejlesztett változatait), amelynek használatát kötelezővé akarják tenni az összes gyártó számára. Nemsokára senki sem gyárthatja és adhatja majd el termékeit az ISO jóváhagyása és minősítése nélkül.

Az ISO egy globális minőségbiztosítási rendszer, amelyet az International Standards Organization (ISO) (Nemzetközi Szabványügyi Szervezet) adott ki.

Az ISO-minősítés Európában kezdődött az „elit" utasítására. Az elején még önkéntes alapon működött, de hamarosan (5 éven belül) kötelező lesz a világon való kereskedéshez. A cégeknek minősíteniük kell majd magukat a világpiacon való életben maradáshoz. A világ legtöbb országa már elfogadta az ISO szabványait minőségbiztosítási rendszereiben. Az ISO a világ termékpiacai ellenőrzésének egyik eszköze már most, és meghatározó szerepe lesz az elkövetkező években és évtizedben.

CHIPKÁRTYÁKáosz

Kártyazűr

Mindannyiunknak van, vagy láttunk már bankkártyát, kártya formátumú személyi igazolványt és más, személyes adatokat tároló plasztiklapot. Az információ egy része a kártyára van nyomtatva és látható, mint például a tulajdonos fényképe, neve, aláírása, címe vagy egy vonalkód. Az adatok legnagyobb része azonban a kártyán levő mágnescsíkban vagy mikrochipben van tárolva, illetve kiolvasható adatbázisokból, ha a kártyát egy kártyaolvasón vagy szkenneren keresztül „hozzákötjük" az adott számítógéprendszerhez.

Mi csak a kártyán levő látható szöveget tudjuk elolvasni. Azt nem tudhatjuk, hogy mit tárol rólunk a mágnescsík, mikrochip vagy az adatbázis, és nem is mondják meg nekünk, mert tudják, hogy rettenetesen megharagudnánk magántitkaink megsértése miatt. A chipkártya (más néven: intelligens kártya, smart card) a legfejlettebb plasztikkártya: több ezer oldalnyi adatot tud tárolni a beépített mikrochipben.

A chip lehet egy memóriachip vagy egy mikroprocesszor. A chipkártyák és a kártyaolvasók vagy más készülékek közötti adatátvitel szempontjából megkülönböztetünk érintkezős, érintkező nélküli és kombinált chipkártyákat. A mikroprocesszoros chipkártyák multifunkciósak is lehetnek, azaz többféle feladat elvégzésére alkalmasak. Egyes chipkártyákon mágnescsík is van. A memóriakártyákba memóriachip van ágyazva, és a floppylemezekhez hasonlóan adatokat tárolnak, melyek leolvashatóak és meg-

változtathatóak külső készülékek segítségével. Ezek a kártyák nem képesek adatfeldolgozásra.

Az első chipkártyák értéket tároló memóriakártyák voltak. Európában kerültek bevezetésre a nyilvános telefonok használatához. Az értéket tároló kártyák bizonyos kezdőösszeggel kerülnek forgalomba, mely minden használat után csökken. Elektronikus pénzt tárolnak, amely tulajdonképpen a memóriachipben levő számokból áll. Ezek a kártyák eldobható, illetve utántölthető változatban készülnek.

Az új lézerkártyák, azaz optikai memóriakártyák az optikai adatrögzítés technológiáján alapulnak. Több megabytenyi, különféle, digitálissá alakított adatot tárolnak, mint például szöveg, kép, hang, zene, szoftver. Ezt a technológiát használják fel a jövőben a legális audiovizuális üzletben az illegális „kalózkereskedelem" visszaszorítására, másolásvédett CD, DVD chip formátumok piacra dobásával. Kedvenc filmjeinket, zeneszámainkat körömhegynyi méretű chipkártyákon vásárolhatjuk majd meg, és berakva a lejátszók kártyafogadó részébe máris a kívánt, legtökéletesebb minőségben hallhatjuk és láthatjuk azokat.

A rendszer képes arra is, hogy megkülönböztesse a tényleges első vásárlót (jogos tulajdonosát és használóját, aki fizetett érte) a második, harmadik és a sokadik gazdájától, akik használni szeretnék, de nem tudják, mert az idegen lejátszókban már nem aktiválhatók. Hasonló az eljárás a mobiltelefonoknál, amikor a SIM kártya hozzá van rendelve az adott készülékhez, idegen készülékben nem aktiválható. A hozzárendelés az első aktiváláskor történik automatikusan, így nem kerülhető ki. Természetesen, mint minden más területen, itt is elindul majd a dekódolás kifejlesztése. Ezzel a feladattal mindig is külön „iparág" foglalkozott – a másik oldalon.

A mikroprocesszoros chipkártyákba a számítógépekhez hasonlóan mikroprocesszor van építve, és nem csak az adatok tárolására, hanem azok feldolgozására is képesek. A chip neve SPOM (self-programmable one-chip microcomputer), azaz egychipes önprogramozó mikroszámítógép. A mikroszámítógéphez operációs rendszer is tartozik, mint például a Windows for Smart Cards.

A chip adatok tárolására és frissítésére, valamint számolások elvégzésére és döntéshozásra is képes, külső készülékekkel is tud „beszélgetni". Ezek a kártyák annyi információt tárolnak és dolgoznak fel, hogy képernyő és billentyűzet nélküli miniatűr számítógépeknek tekinthetők. De mivel annyira aprók, az emberek általában nem veszik figyelembe az erejüket. Pedig nem ártana! A chipkártyák a tulajdonosaikról tárolnak személyes adatokat, tehát olyanok, mint valami apró kémek a zsebben. És ki akar magával hordozni kémeket?...

Az érintkezős chipkártyák csak úgy tudnak külső készülékekkel és számítógépekkel „beszélgetni", ha kártyaolvasókba helyezik őket. Az érintkező nélküli chipkártyákba viszont egy apró rádió adó-vevő van ágyazva, mely jelekkel kommunikál a kártyaolvasókkal vagy más készülékekkel, és ehhez nem is kell őket a pénztárcából vagy a táskából elővenni.

A hibrid vagy kombinált chipkártyák egy kontaktchippel és egy rádió adó-vevővel is fel vannak szerelve, hogy érintkezős és érintkező nélküli tranzakciókat is elvégezhessenek. Ezek a mikroprocesszoros chipkártyák többféle feladatot tudnak elvégezni, mint például azonosítás, belépésellenőrzés, pénzügyi, törzsvásárlói, egészségügyi és más alkalmazások. A bankkártya-kibocsátó társaságok, bankok és high-tech vállalatok összefogtak, hogy a világon forga-

lomban levő plasztik bankkártyákat mikroprocesszoros chipkártyákkal váltsák fel. A pénzkiadó automatákat (ATM) és a kártyaelfogadó helyeket (POS-terminálokat) chipkártyák elfogadására alkalmassá alakítják át.

Már több százmillió chipalapú terheléses és hitelkártya, valamint elektronikus pénztárca használatos világszerte. Ezeknek egy része más szerepet is ellát, például törzsvásárlói kártya, digitális személyazonosító és elektronikus kulcs épületekbe való belépéshez. Több mint 100 millió elektronikus pénztárca van forgalomban csupán Európában. Az Europay International által kibocsátott új, nemzetközi elektronikus pénztárca neve Clip. Franciaországban 37 millió chipalapú bankkártya van, azt tervezik, hogy olyan chipkártyát bocsátanak ki, melyek elektronikus pénztárcaként, terheléses és hitelkártyaként, valamint törzsvásárlói kártyaként és elektronikus utazási jegyként fognak működni, ráadásul a számítógépes hálózatokhoz való hozzáférést is szabályozzák. Belgiumban terheléses chipkártyával rendelkezik több mint 7 millió személy. Majdnem minden terheléses kártyán mágnescsík és chip is tárolja az adatokat. A kártya elektronikus pénztárcaként is szolgál.

Azt tervezik, hogy online vásárlás esetén a tulajdonos azonosítására is felhasználják a chipet, ezért PC-khez kapcsolható chipkártyaolvasókat szándékoznak eladni a kártyabirtokosoknak. Horvátországban 27 bankból álló konzorcium azt tervezi, hogy a mágneskártyáról áttér elektronikus pénztárcát, terheléses és hitelkártyát magában foglaló chipkártyákra. Az American Express Blue (Kék) hitelkártyája az első országos chipkártya az Egyesült Államokban. A kártyán levő mágnescsík tárolja a hitelfunkciót, a chip

meg a kártyabirtokos digitális személyazonosságát. Később más szerepekre is alkalmassá fogják tenni a chipet.

A Visa 22 millió, a MasterCard pedig 14 millió mágnescsíkos hitelkártyáját chipkártyára szándékozik kicserélni Kanadában. Mexikói bankok a 30 millió mágnescsíkos terheléses és hitelkártyát chipkártyákra fogják kicserélni. Később multifunkciós kártyák bevezetését tervezik, melyek elektronikus pénztárca, hitel, terhelés és törzsvásárlói alkalmazásokat fognak tartalmazni. Brazíliában a 11 millió Visa hitelkártyát és a 15 millió Visa terheléses kártyát folyamatosan cserélik ki mágnescsíkot is tartalmazó chipkártyákra. A brazíliai MasterCard-kibocsátók is át akarnak térni a mágneskártyákról a chipkártyákra. Dél-Koreában chipalapú Visa hitelkártyákat kezdtek kibocsátani, és olyan alkalmazásokat tesztelnek, mint törzsvásárlói programok, terhelés és elektronikus kereskedelem. A MasterCard International chipalapú hitelkártyákat vezetett be Szöulban.

Az emberek még mindig készpénzzel szeretnek fizetni, ezért a bankok különféle meggyőzési módszerekkel próbálkoznak, hogy rávegyék őket a kártyák használatára. Az elektronikus pénztárcának nevezett banki chipkártyát, amely „elektronikus pénzt" tárol a beépített mikrochipben, úgy mutatják be, mintha különbözne a többi bankkártyától.

Ne felejtsük el, hogy a cél a készpénz teljes kiiktatása, ugyanis annak a mozgása nem hagy nyomot, és olyan fizetőeszközzel való helyettesítése, amelynek útját és a vele fizető személyeket nyomon lehet követni. A két fizetési módszer között a következő a különbség: terheléses és hitelkártyák esetén a fizetendő összeget levonják a vásárló bankszámlájáról, és átutalják az eladó bankszámlájára, ami

tulajdonképpen azt jelenti, hogy néhány, számítógépen tárolt szám megváltozik.

Elektronikus pénztárcák esetén a kártyán levő chipet először feltöltik „elektronikus pénzzel" a kártyabirtokos bankszámlájáról, ahonnan az összeget levonják, azaz a kártyán levő chipben és egy számítógépen bizonyos számok megváltoznak. A kártyával való fizetésnél újra csupán számok változnak meg, ezúttal a chipben és az eladó bankjának számítógépén. Vagyonunk lassan átalakul számítógépeken tárolt számokká, melyeket át lehet írni vagy ki lehet törölni akár örökre is. Bárhogyan is nézzük, valódi készpénz nem fordul elő a fenti két eset egyikében sem.

A készpénz esetében azonnal tudjuk, hogy rendelkezünk-e a megfelelő pénzösszeggel, a virtuális pénz esetében viszont soha nem fogjuk tudni, hogy a tranzakció során lesz-e elegendő vagy sem. Megszűnik a feketepiac, a csencselés, mert nem a készpénz lesz a tényleges fizetőeszköz. Nem lesz alkudozás, a „virtuális pénzhamisítás és pénzmosás" meg csak azoknak adatik meg, akik a központi terminálokat, a szervereket kezelik, és a pénzforgalmat, a pénz áramlását szabályozzák. Az átlagember meg hálát adhat Istennek, ha egyáltalán lesz valamilyen fizetőeszköz-adatsor a chipkártyáján, amivel a napi szükségleteit ki tudja elégíteni.

Azt ajánlom a tisztelt olvasóknak, hogy amíg még van és lehet, rakjanak el emlékbe néhány most használatos bankjegyet, hogy pár év múlva meg tudják mutatni az unokáiknak, milyen is volt a pénz, amely meghatározta az életminőségünket. De az eljövendő kornak voltak már előhírnökei, mint például a világháborúk alatt és utána kitört inflációk, gazdasági összeomlások, amikor jegyre lehetett kapni mindent az üzletekben, mert az aktuális pénznek

nem volt értéke. A jegyre megszabott mennyiségű és minőségű árut lehetett venni, hiába szerettünk volna mást vásárolni. Ez minden esetben kiszolgáltatottságot jelentett és jelent majd a jövőben is az emberiség számára.

A mobiltelefonokban és a nyilvános telefonokhoz több százmillió chipkártya használatos. A GSM (Global System for Mobile Communications, azaz a Mobil Távközlések Globális Rendszere) digitális mobiltelefonok SIM (Subscriber Identity Module, azaz Előfizető-Azonosító Egység) chipkártyákat használnak a felhasználó személyazonosságának a megállapításához.

Állami egészségbiztosítási rendszerrel rendelkező egyes országok azt tervezik, hogy chipkártyákon tárolják majd a betegek adminisztratív adatait és kórtörténeteit. Németországban már chipkártyákat használnak az egészségügyi rendszerben. 80 millió chipkártyát postáztak ki a biztosítottaknak, PC-kkel és chipkártyaolvasókkal szereltek fel több százezer orvost és fogorvost. A mentők hordozható kártyaolvasókat kaptak.

Franciaországban az állami tulajdonban levő társadalombiztosítási szervezet (CNAM) egy „Sésam Vitale" nevű tervet indított el, melynek az a célja, hogy minden állampolgárnak/páciensnek egy mikroprocesszoros chipkártyát osszon ki. A kártya az első fázisban adminisztratív adatokat, a második fázisban adminisztratív és orvosi adatokat (a páciens kórtörténete) tárolna. A gyakorló orvosok azonosító chipkártyákat kapnának, rajta elektronikus aláírásukkal.

A belga egészségbiztosító, a Mutualités Belges társadalmi azonosítási rendszere, a SIS megköveteli a páciensek és orvosok ellátását chipkártyákkal. Így hát az egészségügyi rendszeren keresztül kényszerítik rá az állampolgárokra

a chipkártyákat, mivel mindenkinek szüksége van valamikor élete során egy orvosra.

Ráadásul óriási visszaélési lehetőségeket rejt magában ez a chipkártyás rendszer, ugyanis a kórtörténet számítógépen keresztül bármikor megváltoztatható. A kártya tulajdonosa soha nem tudhatja, hogy személyéről pozitív vagy negatív információkat tárolnak-e személyi adatbázisában. A beteg élete és halála feletti ellenőrzés így illetéktelen kezekbe kerül. Az orvos is könnyen elintézhető, ha nem azt teszi, amit diktálnak neki: elég, ha megvonják vagy letiltják a praktizálásához szükséges kártyáját.

Szöulban egymilliónál több chipkártyát hoztak forgalomba, melyekkel a buszokon lehet fizetni a jegyek és zsetonok mellett. Fizetéskor ezeket a kártyákat nem kell kivenni a pénztárcából vagy a táskából, az összeg úgyis automatikusan levonódik róluk a buszokon felszerelt készülékek segítségével.

Az ausztráliai ERG felszerelte Hongkongban az Octopus (Polip) nevű chipkártyarendszert a vonatokon, buszokon, villamosokon, kompokon való utazáshoz. 10 000 terminálból álló hálózatot hoztak létre, és 8 millió kártyát bocsátottak ki. Az ERG Ausztráliában kísérleti vállalkozásba fogott Bunbury városban, melynek célja az, hogy érintkező nélküli (azaz rádió adó-vevős) chipkártyákkal történjen a fizetés utazáskor. Később esetleg egy elektronikus pénztárcát is beépítenek a kártyába, mely érintkezős módban fog üzemelni. A modern kori jegyellenőrök zsebbe rejtett leolvasókészülékekkel szállnak fel a járművekre, és elvegyülve az utasok között a készülék segítségével érzékelni tudják majd, hogy a közlekedési eszközökön utazók közül ki nem rendelkezik érvényes utazási kártyával. Az ilyen rendszereket lehetetlen kijátszani, mivel két lehetőség

adódik: vagy van kártyája, vagy nincs. Akinél nincs, annál az ellenőr készüléke csendben marad. Ez egy diszkrét, de egyben alattomos eljárás is.

Ezek a fejlesztések nagyon ijesztőnek tűnnek, mert érintkező nélküli, azaz beépített apró rádió adó-vevőket tartalmazó chipkártyákat igényelnek. Nem lehet biztosan tudni, milyen adatokat, kinek, hova és mikor fog sugározni a kártya. Könnyen megeshet, hogy az elektronikus pénztárcát egy távoli személy vagy számítógépprogram titokban kiüríti, mert ezek az érintkező nélküli tranzakciók automatikusan történnek, és még a PIN számunkra vagy jelszavunkra sincs szükség.

Kereskedők, benzinkutak, gyorsétkezdék, szállodák és gépkocsikölcsönzők törzsvásárlói programokat ajánlanak vásárlóiknak. Egyesek közülük chipkártyákat használnak a vásárlók azonosításához. A Boots 5 millió Advantage kártyát bocsátott ki, a Shell pedig több millió Shell chipkártyát számos országban. Chipkártyákat már több éve használnak épületekbe, parkolókba való beléptetéshez, és elektronikus rádió adó-vevős kocsikulcsként az ajtók kinyitásához és a motor beindításához.

Világszerte új, chipkártyás diákigazolványokat vezetnek be az egyetemeken és a főiskolákon. Ezek multifunkciós kártyák, melyeket beléptetésre, pénzügyletekre, a számítógépek és a könyvtár használatára, fénymásolásra, árusító automaták, mosógépek stb. használatára terveztek. Több európai ország felsőoktatási hallgatója új chipkártyás diákigazolványt kapott a közelmúltban, melyeket az országhatárokon kívül is tudnak használni, különböző célokra (olcsó szállások igénybevételére, könyvtárak, múzeumok látogatására, kedvezményes közlekedésre). A Motorola Inc. a Berlini Műszaki Egyetemmel és a berlini köz-

lekedési szervekkel együttműködve egy olyan multifunkciós chipkártyás diákigazolvány kifejlesztésén dolgozik, mely magában foglalna egy automatikus menetdíjfizető rendszert is. Az egyre komplexebbé váló kártyahasználat egyre komplexebb nyomon követést és megfigyelést eredményez.

A világon az első chipkártyás gépjárművezetői engedélyt Argentína egyik tartományában, Mendozában bocsátották ki. Az ottani rendőrök kézi kártyaolvasókkal vannak felszerelve, hogy elolvashassák a kártyán tárolt adatokat a vezetőről és legutóbbi szabálysértéseiről. Ez a technológia egyre nagyobb teret nyer az országok államvédelmi szerveinél és közlekedésrendészeteinél. Az adatokat frissíteni is lehet, ha szükséges. A kanadai Ontario és Quebec tartományok olyan chipkártyákat fejlesztettek ki az állampolgárok számára, melyről nem jelezték, hogy milyen funkciókat töltenek be. Egyszerűen kötelezővé tették a használatukat. Valószínűleg gépjárművezetői engedélyként, társadalombiztosítási kártyaként és sportolói engedélyként működnek majd a jövőben.

Az amerikai nemzetvédelmi minisztérium 2000 októberétől kezdődően 4 millió chipkártyát osztott ki minden aktív szolgálatban levő katonai és polgári személynek, egyes tartalékosoknak és az egyéni szállítóknak, hogy felügyelhessék az épületekhez, kormányzati számítógép-hálózatokhoz és az internethez való hozzáférést. A kártyán egyéb alkalmazások is lesznek, mint például elektronikus pénztárca, leltár, a kiképzések nyomon követése. A többi állami szerv is hasonló funkciókat ellátó chipkártyákat fog folyamatosan kiosztani az alkalmazottainak.

Az egyik amerikai kormányzati szerv az összes köztisztviselőnek azonosító chipkártyát osztott ki Smart Access Common ID névvel. A kártya digitális bizonyítványt tárol, hogy felügyelhesse az épületekhez, számítógépekhez és az internethez való hozzáférést. Más alkalmazások is vannak a kártyán, mint például az alkalmazottak kórtörténete, elektronikus pénztárca, törzsvásárlói programok, leltári adatok és egyéb. Aki a hivatalokban szeretne dolgozni, annak kötelező a kártya használata.

Amerikában az illegális bevándorlás megfékezését célzó törvény részeként pár évvel ezelőtt országos chipkártyás személyi igazolványt javasoltak. Az elképzelés szerint minden amerikai állampolgárt és törvényes bevándorlót elláttak volna egy ilyen igazolvánnyal, és a munkáltatóktól megkívánták volna, hogy a kártyák alapján ellenőrizzék le a dolgozók státusát, megakadályozva ezáltal az illegális bevándorlók munkához jutását. A rendszerhez az állampolgárokat nyilvántartó hatalmas, központi számítógépes adatbankok létrehozását javasolták. Állami segélyeket is csak a kártyák felmutatása után utaltak volna ki. Kártyaolvasóba helyezve ezt a vonalkódos, biometrikus, mikrochipet tartalmazó azonosítási kártyát, tulajdonosáról olyan, számítógépeken tárolt adatok váltak volna elolvashatóvá, mint például családi állapot, gyerekek, kórtörténet, munkahelyi adatok, lakás- és személygépkocsi-tulajdonjog, közlekedési feljegyzések, bankügyletek stb.

Mikor ezen országos személyi igazolvány javaslatának híre megjelent az újságokban, az amerikaiak tiltakozása olyan szintet ért el, hogy a kártya bevezetését „elhalasztották". Vajon mi késztette az amerikaiak nagy többségét a felháborodásra? Az, hogy tudták, ez még fokozottabb ellenőrzéshez vezethet. Mivel mindenkire kiterjedő és teljes ellenőrzést csak egy rendőrállam bürokráciájával lehet elérni, az utóbbi években fokozódott egy kártya formátumú

országos személyi igazolvány bevezetésére való törekvés. Egy országos személyazonossági adatbázis jelenti a polgári szabadság lejtői közül a legmeredekebbet és a legsíkosabbat.

Az a rendszer, amely több tízezer kormánytisztviselőt és ügyintézőt alkalmazna, és amelynek a létrehozása és működtetése több tízmilliárd dollárba és euróba kerülne, nem korlátozódna csupán az illegális vendégmunkások felderítésére. Miért ne használnák, gyakorlatilag többletkiadás nélkül, mondjuk a fontos személyek követésére is? Ki merne ez ellen tiltakozni vagy ellenkezni? Miért ne követhetnék azután az elítélt, büntetésüket letöltött gyilkosokat is? És az erőszakot elkövetőket, a kábítószer-kereskedőket, a dílereket, a kábítószerfüggőket? És általában a gonosztevőket. A gyerektartási díj fizetésével elmaradt apákat, vagy az adócsalókat. Netán a „politikai szélsőségeseket". Sőt, a „vallásos szekták" tagjait. A szexuálisan degenerált és aberrált fanatikusokat. Az AIDS-vírus hordozóit. A fegyverkereskedőket és a fegyverrel rendelkező személyeket. Minden politikai fordulat után a bal- meg a jobboldal hozzáadná saját kedvenc társadalmi ellenségeit a megfigyelési listához. Egészen addig, amíg végül minden ember el nem foglalja a maga helyét a központi adatbázisban a neki kijelölt fájlban.

Sokakat aggaszt (többek között engem is!), hogy a kártyákat nem csak a mi biztonságunk érdekében, a bűnözők és a terroristák kiszűrésére használnák, hanem valószínűleg egy rendőrállam létrehozására is, hogy a már amúgy is bekerített lakosságot még közelebbről szemmel tarthassák. Erre azért törekednek az államok, hogy egyre jobban kiterjesszék hatalmukat, és az emberek fölött totális hatalmat építsenek ki. Az azonossági kártyát a beültethető mikro-

chip lehetséges elődjének, valamint a kommunisták és a nácik által kért „megkülönböztető papírok" utódjának tekintik.

A brit parlamentnek 2004. november 29-én bemutatott, „The Identity Cards Bill" névre hallgató törvényjavaslat elfogadásával a kormány egy biometrikus azonosítókat tartalmazó chipekkel ellátott személyazonossági kártyarendszert vezetne be 2010-ig. A „National Identification Register" elnevezésű, gigantikus adatbázisban tárolásra kerülő információk között szerepelnének az állampolgárok nevei, címei, valamint olyan biometrikus adatok, mint az ujjlenyomat, az arc és az írisz jellemzői. A javaslatot, melynek megvalósítása 5,5 milliárd fontba (10,3 milliárd USD) kerülne, a brit alsóház 224 a 64-hez arányban szavazta meg. A tervek szerint 2012-re a biometrikus útlevél mellett valószínűleg egy különálló biometrikus személyi kártya használata is kötelezővé válik majd valamennyi brit állampolgár számára, beleértve a gyerekeket is. Nagy-Britannia körülbelül 60 milliós népességű, ezért nem nehéz kiszámolni, hogy ez mekkora üzlet egy behatárolható kis csoportnak, akik kezükben tartják ezt a piacot. Ezek a kis csoportok (sejtek) a világ összes országában jelen vannak, szoros köteléket alkotnak, és függőségi viszony van közöttük. Nem nehéz elképzelni, hogy ez az érdek-összetartozás (néhol alárendelt) milyen változásokat fog okozni az életünkben rövid időn belül.

A javaslat jóváhagyásának napján az Egyesült Államok Képviselőháza megszavazta az ID-kártyás rendszer saját verzióját, 261:161 arányban. Az amerikai „Real ID Act" megkövetelné, hogy minden egyes kiállított jogosítványt és egyéb, személyazonosságot igazoló okmányt fizikai biztonsági adatokkal lássanak el, mint például az arc jel-

lemzőinek digitális fényképe – mindezt gépekkel leolvasható formában, így akár még egy mágnesszalagot vagy RFID (radio frequency identification) címkét is magukba foglalnának az új kártyák.

Már most is komoly problémákat okoz a bevezetése, mert az államokban élő és kendőt viselő muszlim nőket kötelezni akarják arra, hogy fedetlen arcukról készített fotókat biztosítsanak a hatóságok részére, az új igazolványok elkészítéséhez. Ezt viszont a vallásuk tiltja. Ebből még komoly bonyodalmak is származhatnak a törvényhozóknak. Jelen pillanatban csupán a szemük látszik az azonosító kártyán. De van olyan is, amelyiken még az sem, csak a fátyol. Ez nagyon vicces, mert majdnem mindegyik kép egyforma, és nem lehet tudni, hogy kit takar a fátyol. Lehet, hogy egy arab terrorista férfit...

Tony Blair miniszterelnök és Charles Clarke belügyminiszter nyilatkozatai szerint a biometrikus azonosító kártyák létfontosságúak a személyazonosság elleni visszaélések, az illegális munkavállalók, bevándorlók és a terrorizmus elleni harcban, valamint kulcsszerepet játszanak az olyan programokkal való visszaélések megfékezésében, mint amilyen az Országos Egészségügyi Szolgálat (National Health Service – NHS). Az adatok manipulálásával komoly pénzeket vehetnek ki a kormányok kincstárából. A brit munkáspárti kormány jelezte, hogy szeretné még a májusi nagy választások előtt törvénybe iktatni az ID-kártya-törvényt. Az ok, amiért ezt az intézkedést nem csupán a kormány, hanem a rendőrség és a biztonsági szervek is támogatják, az, hogy az emberek úgy vélik (különösen a biometrikus útlevelek és a biometrikus technológia elérhetővé válásával), egy olyan, személyi azonosságot igazoló kártyát tudnak megalkotni, amely a lehető legnagyobb védelmet nyújtja a terrorizmus és a bűnözés ellen.

Az angolok első számú vezetője nem hiszi, hogy a kártya bevezetése helytelen lenne, vagy hogy sértené bárki jogait. A legtöbb ember amúgy is hordoz magával valamilyen, azonosságra utaló okiratot. Igen ám, de amíg ez az okmány egy sima papírigazolvány, addig nincs is semmi probléma, de amikor ez átalakul egy bárhonnan, bárki által ellenőrizhetővé váló igazolvánnyá, akkor már jogos az aggodalmunk. „Véleményem szerint ez már rég időszerű lett volna, most pedig bele kéne vágnunk, és túl lenni rajta minél előbb" – mondta egy parlamenti felszólalásában Tony Blair miniszterelnök. Vajon egy ilyen kijelentéssel egy államfőnek ez a valódi célja? Vagy csak én gondolom másként?! Nem hiszem! Clarke ennek ellenére jelezte, hogy a törvényjavaslat ellenállásba ütközhet a brit felsőházban. A „The House of Lords – A Lordok Háza" a második a brit kormány két parlamenti háza közül, és hatalmában áll megállítani egy, az alsóház által már elfogadott rendelkezést. Viszont Nagy-Britannia már döntött arról, hogy az elkövetkezendő években minden egyes új brit útlevélbe az arc azonosítására alkalmas adatokat tartalmazó chipek fognak kerülni.

Egy 10 000 önkéntes segítségével lefolytatott, hat hónapos biometrikus próbafutamot nemrég befejező „The U. K. Passport Service" (UKPS) ezután ezt a technológiát vinné tovább a személyazonosító kártyarendszer kialakításánál. A próbát végző cég három biometrikus azonosítótípust tesztelt: az elektronikus ujjlenyomatot, az írisz rögzített képét, valamint egy teljes arcletapogatás adatait. Az Atos Origin a teszthez szükséges hardver és szoftver leszállításáért és üzembe helyezéséért felelt; az NEC az ujjlenyomat-

azonosító rendszert; az Identix az ujjlenyomatok rögzítéséhez, valamint az arcok összehasonlításához használatos technológiát, az Iridian Technologies az íriszfelismerési technológiát szolgáltatta. Ezek a cégek mind-mind a „Big Brother Művek" területén dolgoznak lázas igyekezettel.

A kormányok biometrikus technológiák hatékonyságába vetett bizalma ellenére egyes bankok és hitelkártyacégek még nem döntöttek a használata mellett, éppen a technológia pontatlanságára hivatkozva. „Úgy találtuk, hogy a téves azonosítások száma még mindig túlságosan nagy – mondta Johan Gerber, a MasterCard International kockázati termékrészlegének felelős igazgatóhelyettese. – Még korainak tartjuk a technológia bevezetését." Azt hozzátette Gerber, hogy a MasterCard érdekelt a jövőben a biometrikus technológia alkalmazásában, és sokkal kisebb léptékben már alkalmazza irodáinak néhány rendszeres látogatója esetében. A MasterCard az egész világot behálózza, ezért is nem áll be még a sorba, hanem kivár, és amikor már mindenki rá lesz kényszerítve a kártyák használatára, akkor jön majd ki a saját fejlesztéseivel, hogy még nagyobb profitra tegyen szert. Ez egyfajta üzletpolitika és taktika.

Az olyan csoportok, mint az angol és walesi ügyvédek számára szakmai közeget jelentő „The Law Society" már kifejezték aggodalmukat aziránt, hogy túl nagy elvárásokat támasztanak az ID-kártya programmal szemben, és hogy a belügyminisztérium nem bizonyította be, hogy a rendszer alkalmas a személyazonossággal való visszaélések visszaszorítására. A biztonsági szakértők pedig arra hívták fel a figyelmet, hogy egy ilyen masszív adatbázis rendkívül csalogató célponttá válhat a hackereknek, a terroristáknak és egyéb bűnözőknek. Egy szakmai elemző

úgy véli, a törvényjavaslat nem tartalmaz óvintézkedéseket a rendszer hatékonyságára nézve, és nem biztosítja az állampolgároknak a róluk tárolt információk helyességének ellenőrzését.

Richard Allan, az angol parlament tagja, valamint a Tudományos és Technológiai Parlamenti Hivatal igazgatótanácsának elnöke ellenezte a törvényjavaslatot, mert túl kiforratlannak és költségesnek tartja. Allan több parlamenti technológiai csoport tagja: az Internet Group-ban és az eDemocracy Group-ban is rendelkezik székkel. „A biometrikus technológiában olyan sok az ismeretlen, hogy pillanatnyilag felelőtlenség lenne elfogadni a törvényjavaslatot" – olvasható Allan webnaplójában. Ennek ellenére az angol törvényhozás a napokban mégis elfogadta a biometria felhasználását, a terrorizmus visszaszorítása érdekében. Ügyészi és bírói engedély nélkül már a gyanú esetén is alkalmazhatják a nyomkövetést, a folyamatos megfigyelést, lehallgatást. Ez az eset is mutatja, hogy az állampolgároknak nem sok beleszólásuk lesz a jövőben az ilyen eszközök használatába. A nagy nyilvánosságot kihasználva, szinte észrevétlenül válnak életünk részévé ezek a technológiák.

ELEKTRONIKAtasztrófa

Technikai támadás

Ma már nincsenek ártatlan technológiák. Mindegyik technológia használata egy „fausti-ördögi" alku, hiszen ezen újítások igénybevételével mindig nyerünk bizonyos dolgokat, míg másokat elveszítünk. Ezért nem árt, ha minden helyzetben végiggondoljuk, hogy mit kapunk, és miről mondunk le egy domesztikált ketyere használatával. A műholdas és kábeltelevíziós szolgáltatók is használnak chipkártyákat az előfizetők azonosításához és elektronikus „pay-per-view (fizeted és nézheted)" fizetéshez. Az USA-ban kicserélték az összes analóg beltéri egységet, és az új egységeket két chipkártyaolvasóval szerelik fel: az egyiket chipalapú bankkártyák, a másikat pedig az azonosító kártyák számára. A modemek a központból ki- és bekapcsolhatók, tehát online kapcsolatban vannak egymással.

Így működnek az országos lefedettséggel rendelkező kábeltelevíziós szolgáltatások is. A modem ott van a lakásokban és a hálószobákban. Mi van, ha azon keresztül észrevétlenül le tudnak bárkit hallgatni? Márpedig a rendszer képes erre! Egyszer is eltöprengtek azon, hogy hol van annak az optikai kábelnek a másik vége, és kik ülnek ott? Szerintem nem, mert olyan természetes a számunkra, hogy bedugunk egy kábelt valahová, és máris nézhetjük a tévét, vagy csatlakozhatunk az internetre.

Kezdjük azzal, hogy bejelentem az igényemet. Megadom a nevemet, a címemet. Eltelik egypár nap, felhívnak, kijönnek és beüzemelik a modemet. Fél óra múlva működik is a rendszer. Egészen addig, amíg rendesen fizetem a

szolgáltatási díjat. Ha módosítani kívánom a csomagot, már ki sem jönnek, mert ezt központilag meg tudják változtatni. De mi történik akkor, ha a személyem állambiztonsági szempontból fontos, és le van adva a szolgáltatónál a nevem? Akkor hozzám nem a szolgáltató szakemberei jönnek ki, hanem mondjuk valamelyik állambiztonsági szerv specialistái. Mert a szolgáltató értesíti az őket is felügyelő szervet, hogy megjelent a nevem az igénylők listáján. A folytatást már el tudják önök is képzelni.

Ha például önre telefonálnának, hogy egy bizonyos időpontban tartózkodjon otthonában, mert valami zavart észleltek a rendszerben, és meg kell, hogy vizsgálják, beengedné a hibaelhárítókat? Hát persze, mivel ők a tulajdonosai a rendszernek. De ki mondja meg, hogy tisztességes szándék vezérli-e őket, vagy ártani akarnak?

A szakember meg tudja állapítani, hogy a modem preparált vagy sem, de ahhoz szét kell szednie a beltéri egységet, (ám akkor megszűnik a jótállás), és láthatóvá válik, hogy valaki belekontárkodott-e a készülékbe. Egy átlagos felhasználó csak azt látja, hogy villog vagy nem. Azt javaslom, hogy áramtalanítsák (minden vezetéket húzzanak ki belőle), ha nem használják. Ha szükség van a használatára, akkor meg intim, illetve fontos dolgokról ne pont a modem közelében beszélgessenek! Vagy tegyenek egy felhangosított hangszórót a modem közvetlen közelébe, heavy metal zenével. Ez is biztos védekezés egy illetéktelen lehallgatás ellen.

De ilyen problémákat vetnek fel a beléptetőrendszerek, a mozgásérzékelők és a kamerák is. Egyes őrző-védő cégek a ház vagy lakás távfelügyeletét ígérik számítógépes biztonsági rendszerek segítségével. Egy sor helyszíni füst- és tűzjelzőt, mozgás- és más érzékelőt, valamint rejtett

videokamerát helyeznek el a lakás helyiségeiben. Ezek a készülékek jeleket küldenek a távfelügyeleti központba telefonon, széles sávú interneten vagy ISDN-vonalon keresztül, esetleg rádióhullámok útján. A reklámokban az áll, hogy a megrendelők nyugodtan elmehetnek otthonról, mert valaki vagy valami majd figyeli a lakását és őrzi értékeit. A rablóról vagy a gyerekkel rosszul bánó pótmamáról videofelvétel készül, tűz esetén riasztják a tűzoltókat, és még rengeteg hasznos dologgal kecsegtetik. De hogyan lehet valaki biztos abban, hogy nem nézik őt is a lakásában, amikor otthon tartózkodik? Aki a lakásába ilyet telepít, az feladja magánéletének utolsó bástyáját: az otthonát is.

Az otthonunkba telepített modern eszközökről a szakemberek csak annyit árulnak el, amennyire szerintük szükségünk van, viszont (egytől egyig) mind magukban hordozzák azt a veszélyt, hogy észrevétlenül figyelhet bennünket bárki anélkül, hogy mi tudnánk róla. A modern integrált rendszerek tulajdonsága, hogy minden adatátviteli (hang, kép) opció bele van már építve a készülékekbe, (az egyfunkciós készüléket nem is lehet eladni a piacon). A mozgásérzékelőben benne lehet egy mikrofon vagy egy miniatűr kamera. A kamerának látszó eszközben sem veszünk észre egy mikrofont. A mindenki által ismert füstérzékelők ideális helyet biztosítanak a mennyezeten a minikameráknak és a szuperérzékeny mikrofonokkal ellátott lehallgatókészülékeknek.

A rafináltság abból ered, hogy a szimpla eszközöket ugyanolyan áron kínálják, mint a már mindentudó rendszereket, ezért a vevők inkább a több lehetőséget kínáló eszközöket vásárolják meg. Ezzel megkönnyítik a telepítők dolgát, akik észrevétlenül beüzemelik az összes opciót anélkül, hogy a megrendelő erre engedélyét adta volna.

A rendszer működésekor a tulajdonos semmi különöset nem fog tapasztalni. Minden úgy működik, ahogy ő kérte. De nem árt megvizsgálnunk közelebbről a lassan fölöslegessé váló hálózati telefont is, amit már eleve úgy reklámoznak, hogy a közvetlen használata nélkül is figyeli a környezetét, amikor a tulajdonos nincs is otthon (és ennek még örülnek is sokan!). Az biztos, hogy ha ingyen adnák, nekem akkor sem kellene!

Bevált szokás, hogy az állami hírszerző szolgálatok kis magáncégeket bíznak meg a telepítésekkel, mert ha „bukta van", vagyis kiderül a turpisság, ezeket a cégeket fel tudják áldozni úgy, hogy ők tiszták maradnak. A kiszemelt cégek kapnak egy ajánlatot: vagy „beállnak a sorba" és vállalják az alantas munkát, vagy korlátozzák a működésüket, folyton zaklatják őket, és lejárató kampány keretében elvesztik az összes ügyfelüket, vagyis lehúzhatják a rolót. A cégek általában beállnak a sorba, és vállalják az együttműködést a szakszolgálatokkal. Sőt, arra apellálnak, hogy ebből a kapcsolatból nekik csak hasznuk származhat. Közben egy életre sarokba lettek szorítva, miután az első megbízásukat teljesítették.

Az is általánossá vált, hogy volt céges profik alapítanak magáncégeket, akiknek már úgyis mindegy, mert ha akarnának, se tudnának kiszállni a „körhintából". Ők lelkiismeret-furdalás nélkül vállalják a „piszkos munkát", amit kenyéradó gazdájuktól kapnak. Ez nem csak Amerikában bevált szokás, hanem az európai országokban és más kontinenseken is.

Ha mégis beengedtük az állítólagos biztonsági szakembereket a lakásunkba (nagy hiba!), akkor soha ne hagyjuk őket egyedül mozogni, figyeljük a ténykedésüket, és minden eszközt, amit be akarnak üzemelni, ellenőrizzünk le!

Elképzelhető, hogy nem tetszik nekik az óvatosságunk, megsértődnek a bizalmatlanságunkon, akkor nyissuk ki a bejárati ajtót, és köszönjünk el tőlük angolosan! De ha maradnának, akkor mindenre figyeljünk, vegyük kezünkbe a kicsomagolt eszközöket! Keressünk rajtuk gombostűfejnyi nyílásokat vagy szokatlan eltéréseket! Előfordulhat, hogy megmutatnak egy szétszerelt „tiszta" eszközt, de a telepítésnél egy preparált eszközt üzemelnek be.

A folyamatos felügyelet időigényes elfoglaltság lehet, de nagyon hasznos! Előfordulhat az is, hogy az első fázisban, felmérésre hivatkozva aprólékosan szemügyre veszik a terepet. Feltűnés nélkül jegyzetelgetnek, méregetnek, bekukkantanak minden apró helyre, arra hivatkozva, hogy a legoptimálisabb lehetőséget ajánlják majd a tisztelt megrendelőnek.

Megjegyzik az egyes eszközök típusait (hifi, tévé, telefon, óra, konnektorok, kapcsolók, lámpatestek és más technikai eszközök), megvizsgálják az áramforrásokat, hálózatokat, légkondicionáló berendezéseket, és részletes jegyzéket készítenek.

Vannak, akik digitális kamerával is rögzítik a látottakat, a tulajdonosnak meg azt mondják, erre azért van szükség, hogy a letelepítésre kerülő eszközök színben és formában is passzoljanak a lakás vagy az iroda szín- és formavilágához. Igen veszélyes dolog ez! És a gyanútlan, hiszékeny emberek még készségesen asszisztálnak is a „szakembereknek"!

Tudatlanságuk miatt sokan nagy árat fizetnek. Egy ilyen telepítés után olyanná válhat a lakásuk, az irodájuk vagy a házuk, mintha nyitva lenne az összes nyílászáró, és idegenek sétálnának ki-be a helyiségekbe, minden akadályoztatás nélkül. Mintha ők is ott élnének velük egy légtérben, közben lehet, hogy a Föld ellenkező oldalán laknak. A magánéletük forog kockán, amely közszemlére kerülhet, és ismeretlen emberek csámcsoghatnak a legrejtettebb, intim dolgaikon. Remélem, kezdik már érteni az aggályaimat! Amíg nem állt rendelkezésre ilyen fejlett technika, nemigen tudtak volna belopózni a hálószobánkba anélkül, hogy ne vettük volna észre őket. Most meg... Én nem érzem magamat exhibicionistának, mint a valóságshow-k szereplői, ezért nem is szeretném, ha folyamatosan figyelnék a ténykedésemet!

Mivel valódi profikról beszélünk, így a megjelenésük, magabiztosságuk, szakmai ismeretük minden gyanút elfedez a megbízóban, és ő azt hiszi, hogy mázlija van. Ebben a hitében meg is erősítik. Legyezgetik a hiúságát, dicsérgetik, milyen jó ízléssel rendezte be az otthonát. Ezzel „el is altatják" még a minimális veszélyérzetét is. A „szakértők" pedig visszatérve a bázisukra, (főleg, ha beépített személyekről van szó), leadják a szükséges információt valamelyik szolgálatnak, vagy a célszemély konkurensének. A felvett adatok alapján elkészítik a stratégiát, a preparált eszközöket. Ezek ugyanolyanok, mint a tulajdonos eredeti eszközei, de már benne vannak a megfigyelésre használható miniatűr eszközök. Ezekkel visszatérnek a lakásba vagy irodába, és a megfelelő pillanatban kicserélik az eredeti eszközöket az általuk hozottakkal.

Az eszközöket általában, ha nem egyszeri (rövid távú) használatra tervezték, csatlakoztatni kell valamilyen áramforráshoz. De az áramforrást ki is lehet iktatni. Ennek megakadályozására használják például a szünetmentes tápegységeket, amelyek áramkimaradás esetén biztosítják az ideiglenes áramellátást. Ez például ideális hely a lehallgatókészülékek számára. A tápegység többnyire ott van a

számítógép közvetlen közelében, amely a tulajdonos íróasztalán található a telefon mellett, így mindegyik üzleti vagy magánbeszélgetést akadálytalanul továbbítja. Minden ugyanúgy működik ezután is, csak már nem egyedül van a tulajdonos a lakásában vagy az irodájában. Természetesen a beígért rendszert is kiépítik, a megbízó meg örömmel fizet a „biztonságáért". Ha idegent engedünk a lakásunkba, nem árt rögzíteni a memóriánkban a mozgását, a tevékenységét, és miután távozott, vizsgáljuk át a mozgásterét, azokat a helyeket, ahol ült, amerre ment, amihez hozzányúlt!

Egy elemes, egyszerű lehallgató poloska (teljesítménytől függően) 300–500 méterre tudja a hangot továbbítani. Az elem nagyságától függően akár egy héten keresztül is közvetít folyamatosan. A bonyolultabbak már távirányítással is működhetnek. Ezeket csak akkor aktiválják a megfigyelők, amikor a célszemély otthon tartózkodik. A jelenlegi mikrofonok olyan érzékenységűek, hogy bárhová helyezik el a lakásban vagy az irodában, a legkisebb zörejeket is továbbítják: az átlagos beszédhang olyan számukra, mintha közvetlen közelről kiabálnánk beléjük, így a suttogást és a sóhajokat is akadálytalanul felveszik.

A munkám során sok érdekes eszközzel találkoztam. Rendkívül izgalmas feladat, amikor egy addig ismeretlen helyszínen vadászhatok ezekre a kártékony rovarokra. A technika, amit a kollégáimmal használok, képes megtalálni a különböző lehallgatókészülékeket, melyekről a szakértőim 99%-os pontossággal meg tudják állapítani, hogy állami vagy magántelepítésűek. A TV-shop reklámokban is hirdetnek rovarirtó eszközöket, de ezek csak játékszerek, szépen villognak, sípolnak, de egyértelmű pénzkidobás az a 20-30 USD is. Az a fő szlogen, hogy ezekkel a laikusok is százszázalékban megtalálják a poloskákat.

Erre azt szoktam mondani, hogy akit be lehet csapni, azt be is fogják csapni. Ha ezek a hirdetések igazak, akkor a specialisták miért nem használnak ilyen, a sarki fűszeresnél is beszerezhető herkentyűket? Találkoztam már olyan esettel is, hogy pont az elhárítóeszközbe volt beleépítve a lehallgató, amit úgy leárnyékoltak, hogy az egyszerű hordozóeszköz működését nem zavarta. Természetesen a professzionális műszerünket nem lehetett becsapni, egyből kiszúrta. Leleményes ötlet, mert mi sem gondoltuk volna, hogy a hatástalanító eszközön keresztül próbálnak lehallgatni valakit. Ez is azt mutatja, milyen sok lehetőség van arra, hogy gyanútlanul bejuttassanak valaki környezetébe különféle megfigyelőeszközöket.

Akinek valóban van mit rejtegetnie a külvilágtól, az folyamatosan használja a féregirtókat, ezért állandóan magával hordja azokat, így csak ki kell preparálni, és máris kész a kapcsolat. Amikor valaki gyanakodik, hogy őt lehallgatják, mert olyan információk kerülnek vissza hozzá, melyeket titokban kívánt tartani, mindent elkövet, hogy megnyugodhasson. Az ilyen eseteket szeretnék diszkréten kezelni, ezért szűk körben kezd el kérdezősködni, tanácsot kér, hogy ki tudna neki egy eszközt vagy szakembert ajánlani.

Sajnos az esetek többségében mindig lesz egy olyan személy, aki konkurensként léphet föl vele szemben, és megpróbálja kihasználni a helyzetet. Az ilyen személyek kapnak az alkalmon, és máris aktívan segítenek az eszköz beszerzésében. Megszerzik számára a (már preparált), mindent tudó műszert, amitől a személy jobban megbízik bennük, és velük szemben az óvatossága is csökken, hiszen olyan közös titkuk van, amit más nem tud. Az élet már számtalanszor bebizonyította, hogy a legbizalmasabb em-

berek is elvesztették önkontrolljukat és ellene fordultak rokonuknak, társuknak, barátjuknak, sőt a főnöküknek.

Vannak olyanok, akik tudatosan félelmet keltenek a célszemélyben, aki előbb elkezd gyanakodni, és később félni. De olyan is előfordult, hogy teljesen ártalmatlan (kamu) eszközöket helyeztek el sorozatosan a megfigyelni kívánt személy környezetében. Mivel soha nem tudta, hogy éppen melyik a valódi, szakadatlanul dolgoztatta az elhárítókat. Ez hasonlít egy szexuális zaklatáshoz, amikor is egy aberrált őrült kitartóan hívogatja telefonon a kiszemelt áldozatát, és a kagylóba liheg.

Egy valamire való eszköz ára 50 ezer USD, és ez is csak az alap. Ilyet már nem vehet akárki, ezeket nyilvántartják, mert a szakemberek kezében „fegyvernek" minősülnek. Sajnos olyan technika még nem létezik, amely meg tudná állapítani, hogy hová és kinek továbbítják ezek a kis undorító bogarak a beszélgetéseinket. Ha valakinek a lakásában vagy az irodájában ilyet találunk, az igencsak elgondolkodik, hogy kinek állhat az útjában, és miért. Ha állami eszközről van szó, akkor ott hagyjuk a helyén, és a tulajdonosra bízzuk, hogy mit kezd vele. Ha magánszférából való, akkor ki is irtjuk a későbbi tanulmányozás céljából. Az elhelyezésük roppant egyszerű: fel kell ragasztani az asztal lapja alá, vagy be lehet csúsztatni a szekrény vagy a könyvek mögé, rendszerint olyan helyekre, amelyeket ritkán mozgatnak.

Figyeljünk autóinkra is, ha nem csak mi használjuk, vagy idegen is utazik benne! A szervizelés a legveszélyesebb, mert ott észrevétlenül kipreparálhatják, és azt tehetnek bele, amit csak akarnak. A céges autókról nem is beszélve.

Nyugodtan tegye fel a kérdést: Miért lennék én útjában

bárkinek, kire jelentek én veszélyt, ki gyűjthetne rólam információt? Én választ erre nem tudok adni, ön ismeri saját magát. Általában nem a hétköznapoknak élő emberek kerülnek megfigyelés alá. Akik fontos információk birtokában vannak, vagy stratégiai pozíciókban dolgoznak, komoly pénzösszegek fölött diszponálnak, útban vannak valakinek, nem árt, ha figyelnek a környezetükre, mert ők potenciális célpontok. Olyanok is azzá válhatnak, akik most még nincsenek hasonló pozíciókban, de várható, hogy oda kerülnek. Ezekről a személyekről azért gyűjtik az információkat, hogy amikor célszemélyek lesznek, akkor a sarokba lehessen őket szorítani.

Az információ akkor is fontos, ha nem aktuális. Egy régen elkövetett baklövés, amit megfelelően „dokumentált" valaki, az adott pillanatban (a jelenben vagy a jövőben) egy karriernek, egy életnek a végét jelentheti. Az ilyen információkkal még kereskednek is, és a média vagy a konkurencia rá a legjobb vevő.

mOBILlegalitás

Mobil-törvénytelenség

Ha az ön telefonjában van Bluetooth opció, soha ne felejtse el kikapcsolni, ha már nem használja! Mindig mosolygok magamban, amikor kigyúrt maffiózókon és szépfiúkon ott látom a Bluetooth fülest. Azt hiszik magukról, hogy ők a sztárok, közben olyanok, mint egy lőlap a lőtéren. Mindenki, akinek van egy speciális fegyvere, szabadon tüzelhet rájuk. Egy biztonsági szakértő az egyik angol metróállomáson például két óra alatt 336 Bluetooth-telefont észlelt a laptopjával, s ezek közül 77 támadható volt. A brit parlament épületében pedig tizennégy perc alatt 46 bekapcsolt és 8 támadható telefont talált. Mindegyik beazonosítható volt, és észrevétlenül lehetett figyelni az adatforgalmat.

Korunk kiberterroristái felmásznak egy magas épület tetejére, összeszerelik a digitális távcsöves puskájukat, rácsatlakoztatják palmtopjukat, majd célba vesznek egy távoli irodaépületet vagy stratégiai fontosságú közhivatalt. Türelmes várakozással annyi rádiójelet gyűjthetnek össze, amivel feltörhetik a rádiós kapcsolatok védelmét, és elkezdhetnek célba lőni.

Természetesen nem valódi acéllövedékekről van szó, hanem bitekről és byte-okról. A gonosz terroristák nem gyilkosságra, hanem adatlopásra vagy adatpusztításra készülnek, ami a mai üzleti világban egyenlő lehet a kivégzéssel. Az aktív Bluetooth-kapcsolaton keresztül a támadó megszakíthatja a beszélgetést, idegen számokat hívogathat, illetve turkálhat az elmentett adatok között. Amint a gyanútlan felhasználók aktiválják telefonjukon a vezeték nélküli Bluetooth-kapcsolatot, a támadók kézi számítógéppel (laptop) vagy noteszgéppel (palmtop) titokban telefonhívásokat kezdeményezhetnek.

A mobilkalózok ezenkívül az éppen folytatott beszélgetéseket is megzavarhatják, illetve bonthatják a vonalakat, sőt a külső támadók észrevétlenül elolvashatják az érkezett szöveges üzeneteket, majd a tulajdonos nevében leveleket írhatnak és küldhetnek el a címzetteknek. Sőt elérhetik, lementhetik és átírhatják a mobilban elmentett telefonszámokat és a határidőnaplókat, és a meghamisított adatokat ezután a telefon memóriája és a SIM kártya egyaránt hiteles változásként menti el.

Ezt a technikát természetesen a „jó oldalon" (kinek jó, kinek nem jó!) álló államvédelmi szolgálatok is rendszeresen használják. Így ismerhetik meg bizonyos fontos személyek kapcsolatait, ismeretségi köreit, amelyek újabb lehetőséget adnak, hogy minél szélesebb körben kutakodjanak az emberek magánügyeiben. Képzelje el, hogy önnek eszébe sem jutna elkövetni valamilyen bűncselekményt, de valami folytán bekerül a száma egy bűnöző telefonjába, aminek pont leszívják az adatbázisát! Máris úgy tartják nyilván, mint a bűnözőhöz tartozó, illetve kapcsolható személyt. Önt is lehallgathatják, megfigyelhetik, noha semmi köze az ügyhöz. Ez esetben a telefonra igazán ráillik az a meghatározás, hogy „szükséges rossz".

Eddig két vezető mobilcég készülékeiben fedezték fel a fenti biztonsági rést. Azóta az általuk gyártott mobiltelefonokat nagy ívben elkerülöm, erre figyelmeztetem az ismerőseimet is, és maradok inkább az ezen kényelmi szolgáltatásokat mellőző régebbi típusú mobiltelefonok használatánál. A Bluetooth-átvitelt kiaknázó bármilyen támadás

a készüléktől és a helyszíntől függően 10–100 méterig terjedő távolságból lehetséges. Akik ilyen mindent tudó, „intelligens" telefonokkal rendelkeznek, azoknak azt javaslom, hogy csakis biztonságos környezetben aktiválják a szolgáltatást, mindenképpen olyan helyen, ahol nem láthatják, hogy mikor használja a telefont. Az ilyen lehallgatási technika nagyon egyszerű, és sokan ismerik is, ezért nem árt óvatosnak lenni.

A Cabir.H és a Cabir.I program bármennyi készülékre át tudja másolni magát, és mivel folyamatosan újabb áldozatokat keres, működésével blokkolja a normális Bluetooth-csatlakozásokat, a készülék akkumulátorát meg gyorsan lemeríti, mintha kisütötték volna. Amint a támadható célpont a fertőzött telefon közelébe ér, a féreg automatikusan el-, illetve átküldi magát. Ezt a vírust bárki megkaphatja, akinek fogadóképes telefonja van.

A mobilos kártevők általában letölthető játéknak álcázzák magukat, és a legújabb változatok már a vírusirtót is megpróbálják kikapcsolni. A mai modern telefonok tárolókapacitása igen nagy, képesek a bonyolult játékok fogadására és lejátszására, ezért csábító egy újabb játék letöltése és kipróbálása. Pont ezt használják ki a vírusprogramok készítői...

Az ún. intelligens telefonok egyre népszerűbbek, a Symbian operációs rendszert például már több mint húszmillióan használják. Nem is csodálkozhatunk azon, hogy a mobilokon is megjelennek az eddig csak számítógépes környezetben ismert biztonsági problémák. Az utóbbi időkben igencsak elszaporodtak a mobiltelefonokat támadó rosszindulatú kódok, amelyek ráadásul egyre kifinomultabbak. Nem is olyan régen, egy Mosquitos elnevezésű játékban találtak elrejtve olyan „trójait", amely titokban

emelt díjas számokra küldött üzeneteket, így szabadítva meg a telefon használóját (fizetésre jogosult tulajdonosát) jelentős összegektől.

Rövidesen megérkeztek a Cabir első változatai, amelyek még „ártalmatlanok" voltak, és bár igen körülményesen (Bluetooth rádiós kapcsolatot használt) másolta át magát egyik telefonról a másikra, villámgyorsan elterjedt. A Skulls (halálfejek, koponyák) néven elhíresült trójai az első olyan kártékony program volt, amely magában a telefonban is kárt tett: az operációs rendszer ikonjait halálfejekre cserélte le, és a telefonáláson kívül minden funkciót letiltott. Később a szerzők összekötötték e két utóbbi programot, és ezt követően mindkettőnek számos új változata is megjelent.

A vírusok szerzői többnyire olyan nevet adnak a kártékony kódokat tartalmazó telepítőfájlnak, amely alapján a gyanútlan felhasználó azt hiheti, hogy egy mobiltelefonon futtatható játék kalózmásolatát szerezte meg. A jövőben új típusú támadásokra számíthatunk, melyeknek többféle (komplex) hatása lehet, például túlszámlázás, tárolt információk felfedése illetéktelenek előtt, felhasználói adatok törlése vagy lenyúlása. Ez már háború!

Az aktuális mobilapplikációk és hardverek fejlesztési folyamataiban a kelleténél többet áldoznak a „mobil-biztonságra", ami rendkívül költséges. A cégek túl sok erőforrást pazarolnak el a mobil-megoldások biztonsági szempontjaira anélkül, hogy figyelembe vennék: a lánc olyan erős, mint a leggyengébb láncszeme, vagyis az adott telefonkészülék működését szabályozó szoftverek.

Nem arról van szó, hogy a biztonság lényegtelen, sőt. Ám a biztonsági megoldásokat csak a legmegfelelőbb szinteken és helyeken kell beépíteni, figyelembe véve az

egyedi helyzeteket és elvárásokat. Most a cégek a legszigorúbb biztonsági elvárásokat építik be mindenhová, függetlenül attól, hogy mit akarnak valójában megvédeni, mitől és miért. Ez pénzpazarlás.

Miért fektetünk vagyonokat pénzben és időben a mobil biztonsági megoldásokba, arra, hogy atombombabiztos technológiát alkossunk, a legújabb biometrikus azonosítással, a legerősebb jelszavakkal, titkosított adattárolással és kommunikációval, a legösszetettebb algoritmussal, ha a védett információt mindenki számára elérhető helyre rakjuk? Vagy ha az információkat kódolatlanul tároljuk és küldjük el az interneten keresztül, közvetlenül a munkahelyünkről? A valódi igényekhez kell méreteznünk a mobil rendszerek biztonsági szintjeit is, és nem az elképzeltekhez.

Napjainkig több százmillió SIM kártyát adtak el, nagy részét csak Európában. Hol van még a többi kontinens? A megfelelően felszerelt mobiltelefonok rá tudnak kapcsolódni a világhálóra, e-mail, internetes banki ügyintézés és internetes kereskedelem céljából, és mindezt a mi kényelmünk érdekében teszik. Vásárláskor természetesen fizetni is kell. Ezért olyan mobiltelefonokat fejlesztettek ki, melyekbe még egy chipkártya, a felhasználó chipalapú bankkártyája is behelyezhető online fizetéshez. Ezek a telefonok helyettesíteni fogják a számítógépet és a banki terminált. A cél az, hogy minden, mindig, mindenhol a kezünk ügyében legyen.

Ahogy peregnek a percek, észre sem vesszük, hogy a mobiltelefon életünk tárgyi-technológiai főszereplőjévé válik. A különböző helyzetekben újra és újra megjelenik a mobiltelefon. Érdemes végiggondolnunk azokat a társadalmi funkciókat, amelyeket ezekben a helyzetekben a

mobiltelefonok betöltenek. A mobiltechnológia meghatározó részévé vált globalizált világunknak is. A alábbi példa is ezt támasztja alá.

Az időpont: 2001. szeptember 11. New York. Egy eltérített repülőgép utastere. A terroristák felszólítják az utasokat, hogy hívják fel a családtagjaikat és búcsúzzanak el tőlük, mert halál vár rájuk. Ez a parancs nagyon is tudatos volt a részükről, nem az emberiesség vezérelte őket. A terroristák a repülőgépen utazó potenciális áldozataik telefonhívásain keresztül biztosították, hogy kitörjön a pánik, a hatóságok számára pedig ellenőrizhetetlenné és szabályozhatatlanná váljon az információk áramlása. De ehhez most már nem kell feltétlenül eltéríteni egy repülőgépet. A kibertérben mindig lehet találni védtelen eszközhasználókat, akiket fel lehet használni egy hasonló támadáshoz. A későbbiekben erről a témáról bővebben olvashatnak.

Ha a légierő időben felismerte volna, hogy mire készülnek a terroristák, és lelőtte volna a gépeket – mint ahogy a negyedik repülőgép esetében vélhetőleg meg is tették –, akkor a nyilvánosság elé nem tiszta lappal, hanem már a hozzátartozók révén megfogalmazott felvetésekre reagálva, védekező kommunikációs helyzetben jelenhettek volna csak meg. Ebben a tragikus helyzetben, úgy tűnik, a mobiltelefon „ördögien" jól vizsgázott. Azok a sajátosságai, felhasználási módozatai kerültek előtérbe, melyek segítik a horrorral szembeni emancipációt, talán csökkentik az érintettek kiszolgáltatottságát, és enyhíthetik azt a szorongást, amelyet a terroristák őrült fanatizmusa mellett ma már a gonosz céljaik uralma alá hajtott technológia is táplál. Ez a történet is a hálózati alapon működő mellérendelt viszonyok fölényét mutatja a hierarchikusan szerveződő, ellenőrző struktúrákkal és intézményekkel szem-

ben. Korunk most még decentralizált világának és hálózati kommunikációjának – legyen az „ördögi" vagy „angyali" – egyik ideális kiszolgálóeszköze a mobiltelefon, ami nagyban fogja segíteni a totális centralizáció kifejlődését.

Persze az ellenőrző és elhárítórendszerek sem esélytelenek, de ebben a szituációban olyanok voltak, mint eső után a köpönyeg. A high-tech lehallgatóknak egy nap alatt sikerült bin Ladenhez kapcsolható információ nyomára bukkanni, viszont nem világos számomra, hogy a támadások előkészítése a szuper lehallgatórendszerek és a műholdas megfigyelés korában hogyan maradhatott teljességgel titokban. Így ez a fent említett hirtelen siker felveti a dezinformáció (valótlan állítás, elterelés) gyanúját.

Végül is itt a kulcskérdés az, hogy a digitalizált csúcstechnológiák korában hogyan történhetett meg ilyen borzalom, és hogyan kell reagálnunk erre a tragédiára. Amenynyire az információknak hinni lehet, a késekkel felfegyverzett merénylők sem mobiltelefonon, sem rádión nem kommunikáltak egymással. De akár bárkit fel is hívhattak volna egy német cég által kifejlesztett és piacra dobott telefonkészülékkel. A berlini székhelyű Cryptophone cég készüléke valójában egy telefonálásra alkalmas kézi számítógép, amelyre titkosító szoftvert telepítettek. A mobilról kezdeményezett hívásokat csak egy ugyanolyan szoftvert futtató telefon vagy számítógép tudja dekódolni. Bár a vállalat által használt titkosítási szabvány már régóta elérhető a számítógépeken, a kézi eszközök teljesítménye mostanában lett akkora, hogy képesek legyenek hasonló szintű titkosításra.

Az új mobil Európában és a tengerentúlon is vegyes fogadtatásban részesült. Voltak, akik örültek annak, hogy az üzletemberek biztonságosan tudnak majd vállalati titkokról beszélni, mások pedig amiatt aggódnak, hogy az eszközök a bűnözők tevékenységét is elősegíthetik. A titokszférát védelmezők tábora viszont úgy véli, hogy az új készülék nem a terroristákat támogatja, hanem a szabadságjogot védelmezi a hatóságokkal szemben, akik egészen hihetetlen méretekben figyelik állampolgáraik kommunikációját. De az is biztos, hogyha ezek a mobilok nagyon népszerűek lesznek, a kormányok védelmi szervei keményen fellépnek a gyártóik ellen és az eszközök ellen. A vállalat vezetői állítják, hogy a készülékekben nem hagytak hátsó bejáratokat (back door) az állami ügynökségek számára, és nem kötődnek semmilyen nemzeti szervezethez, mint riválisaik. Ez elég hihetetlenül hangzik! Ráadásul ezt a biztonságot mindenki megismerheti, mivel a program forráskódját nyilvánosságra hozták.

A Microsoft Windows operációs rendszert használó telefont a tajvani High Tech Computer vállalat gyártja. A párban eladásra kínált készülék ára mintegy 3500 euró. Az ára miatt valószínűleg nem lesz tömegcikk belőle, de nem is annak szánják. Bankárok, ügyvédek és cégvezetők fogják megvásárolni, olyanok, akiknek a birtokukban lévő információk felbecsülhetetlenül sokat érnek, és hajlandók ennyi pénzt áldozni a biztonságra. A cég szerint a készülék exportját nem korlátozzák, viszont a vásárlóiktól erkölcsi bizonyítványt kérnek. Ezáltal személyhez kötik a használatát. Vagyis: aki megveszi, az egyből potenciális célpontjává válik a nemzetbiztonsági és államvédelmi hivataloknak.

A „levegőből" lehallgatni nem megoldható, mert a célszemély közelében kell lenni, és vele együtt kell mozogni. Szerintem a mobiltelefon az egyik legjobb lehallgatókészülék. Mint minden más, amiben hangszóró és mikrofon

van elhelyezve. Régen és ma is ezért építettek előszeretettel a telefonba (mobilba és vezetékesbe egyaránt) lehallgatóeszközöket. A legnehezebben elrejthető, és a célnak megfelelő méretű mikrofon gyárilag adva van, csak rá kell csatolni az apparátot, ami aztán a környezetünkből mindent közvetít.

Ugyanígy alkalmas a tévé és a rádió vagy a music center hangfala is erre a feladatra. A mobiltelefonban az akkumulátor kivétele után is ott marad a mikrofon. Ha beleapplikálnak egy miniatűr akkumulátoros adót, amit a belehelyezett saját akkumulátor folyamatosan fel is tölt, nyert ügye van a használójának. A Moszad készített olyan telefonokat, amelyeknek akkumulátorjában áram helyett robbanóanyag volt. A tulaj felvette, majd miután azonosították, hogy ő az, aktiválták a robbanóanyagot, és felrobbantották (ártalmatlanná tették) a célszemélyt.

Az ilyen mobil mindenkinek káros! Egy trükk nélküli mobiltelefon (ezt kevesen tudják), a kikapcsolás után is működik (éberen alszik), hiszen érzékeli a bekapcsolási parancsot is. Innen már csak szoftverkérdés, hogy mi fut „A", és mi fut „B" változat alatt. Ezt a módszert olyan bűnözői körök használják, akik nem férhetnek hozzá a központban rögzített adatokhoz. A „biztonságunkért" felelős szakszolgálatoknak állandó „belépőjegyük" van ezekbe a vezetékes és mobiltelefon-központokba, a szolgáltatók jóváhagyásával, de a tudtuk nélkül, ahol időről időre ellenőrizni tudják a célszemélyek beszélgetéseit.

Akinek vaj van a fején, az egész mobiltelefon-arzenált használ. Egy az előfizetéses pizza-, taxi- és nőrendelésre, a többi praktikum, dominó, vagyis anonim (beazonosíthatatlan kártya). A szükséges időpont előtt egy perccel aktiválja a telefont (mivel magát a telefonkészüléket is be

tudják azonosítani), és csak arra az egy beszélgetésre használja. Ettől kezdve lényegtelen, hogy lehallgatják, vagy meghatározzák a helyét.

A feltöltőkártyás svájci mobilfelhasználóknak a jövőben azonosíthatóaknak kell lenniük. A svájci parlament 124 igen és 27 nem szavazattal fogadta el az ezt előíró törvényt, követve a felsőház terrorizmusellenes intézkedésekre tett javaslatait. Ez egy elvontabb szinten is megjelenő problémát vet fel: a digitális kontroll sok mindenre jó, de háttérbe szorítja a nem digitalizált megfigyelést; a csomagátvilágítás ezernyi tárgyat kiszűrhet, de egy ártatlan hengernek látszó bicskát aligha; a szuperintelligens lehallgatórendszerek akár az összes mobilhívást és információs adatforgalmat rögzíthetik, de egy postagalambbal vagy bármely más betanított állattal (delfin, kutya) szemben tehetetlenek.

A mobil megoldásokra szakosodott Phone House fejlesztőcég elsőként kínál mobiltelefonon alapuló nyomkövető szolgáltatást, mely Belgiumban már elérhető. Aki utána kíván járni a partnere vagy a gyermeke hollétének, az interneten megadhatja a mobiltelefon adatait, és azonnal részletes térképet kap az aktuális tartózkodási helyről. A szolgáltatás ára keresésenként egy euró. Németországban már több mint egy éve kínálja a gyermekek felkutatására használható hasonló szolgáltatását egy kis cég. Az aggódó belga szülők immár ellenőrizhetik, hogy a gyermekük csakugyan az iskolapadot koptatja-e éppen. Féltékeny férjek szintén valós időben ellenőrizhetik, hogy a nejük nem csalja-e meg őket.

A helymeghatározási lehetőséggel kapcsolatban kevéssé lelkes a belga Child Focus nevű szervezet, amely elhurcolt gyerekek felkutatását tűzte ki céljául. A szervezet

nagy ismertségre tett szert a gyerekrabló és gyerekgyilkos Marc Dutroux ügyében. „A gyerekek magánszférája drasztikusan sérül, gyakorlatilag pórázra kerülnek" – kritizálta az új lehetőséget a Het Laatste Nieuws belga napilapban Isabelle Marneffe, a Child Focus munkatársa. A Phone House ezzel szemben arra hivatkozik, hogy a célszemélyeknek a szolgáltatásra jelentkezéssel beleegyezésüket kell adniuk a megfigyeléshez. Ez kiskorúakra nem vonatkozik, itt mindenképpen a szülők szava dönt.

A belga adatvédők már félreverték a harangot, és bejelentették a helymeghatározó szolgáltatás ellenőrzését. Ha kiderülne, hogy a Phone House eljárása az érvényes jogelvekbe ütközik, a céget akár 100 ezer eurós bírsággal is sújthatják. A cégek ennek ellenére folyamatosan fejlesztenek, és arra törekednek, hogy minél bonyolultabb eszközöket dobjanak a piacra. A felhasználók nagy többsége úgyis a szolgáltatások általános részét használja ezután is, így a gyártók a szakszolgálatokkal egyeztetve, észrevétlenül belecsempészhetik a készülékekbe az „extra" állami szolgáltatást nyújtó képességeket is. A felhasználás határait viszont nem mi, a felhasználók, hanem a minket figyelő szolgálatok állítják fel.

PRINTERvenció

Kódoló nyomtatók

Tudták, hogy a legtöbb színes lézernyomtató csöndben, szabad szemmel nem látható jelekkel rögzíti a papírra egyedi azonosító számát? Nem valószínű! Pedig ez az eljárás már közel húsz éve létezik, elsősorban az „okmány- és pénzhamisítók egyszerű azonosításában" van szerepe, de a vásárlókat elfelejtették erről tájékoztatni. Tudatosan?! Szakértők szerint a legtöbb nyomtatógyártó cég elhelyezi színes nyomtatóinak és színes fénymásolóinak szériaszámát és gyártási számát minden egyes dokumentumon, amit a gépek kiköpnek. Az USA és más országok bűnüldözői már folyamatosan használják a rejtett jeleket a hamisítók leleplezésére.

A Xerox cég lézernyomtatói, másolói és multifunkciós eszközei minden gép szériaszámát apró sárga pontokba kódolva rányomtatják a papírra. A milliméteres pontok a papír minden négyzetcentiméterén szerepelnek. Ez olyan, mint egy rendszám. A pontok az oldalak összesen kevesebb mint ezredrészét foglalják el, ráadásul sárga színnel kerülnek a fehér papírra, így szabad szemmel nem láthatóak. Ha viszont kék leddel – például egy kulcstartóra akasztható zseblámpával – megvilágítjuk a papírt, nagyítóval már láthatóvá válnak a jelek. A lézernyomtatókkal könnyen lehet dokumentumokat, vagy akár pénzt hamisítani.

A technológia azonban arra is alkalmas, hogy visszakövessenek minden dokumentumot ahhoz a személyhez vagy vállalkozáshoz, amelyik kinyomtatta. Bár az eljárás jó ideje létezik, a nyomtatógyártók nem tartották szüksé-

gesnek, hogy a vásárlókat tájékoztassák róla. Vajon miért?! Lorelei Pagano, az amerikai titkosszolgálat hamisítási szakértője hangsúlyozta, hogy a nyomozó hatóságok csak akkor használják a szériaszámokat azonosításra, ha hamisítási ügyben nyomoznak. „Kizárólag bűncselekmény esetén nyerik ki a dokumentumokból az információkat." John Morris, a Demokrácia és Technológiai Központ ügyvédje ezzel kapcsolatban megjegyezte: „Ez a fajta biztosíték engem nem igazán nyugtat meg. De az a minimum, hogy értesítsék a vásárlókat."

Akit zavar ez a „bevált" gyakorlat, az sem tudja házilag kiiktatni a szerkezetet, és ha megpróbálná, valószínűleg elrontaná a printert. A szerkezet maga egy apró chip a lézer mellett, ami a nyomtatás előtt nagyjából húszmilliárdod másodperccel rögzíti a pontokat. Eddig még senki nem tudta megbecsülni, hogy hány nyomtatóban, másolóban és multifunkciós gépben alkalmazzák az eljárást, de az tény, hogy a nagyobb cégeknél általános annak használata. A hamisítási ügyekben a titkosszolgálat először a nyomtatványok alapján meghatározza a nyomtató típusát és szériaszámát, majd felveszi a kapcsolatot a gyártó és forgalmazó céggel. Némelyik vállalatnak, mint például a Xeroxnak, van vásárlói adatbázisa, és ezt megosztja a kormányszervekkel. A Xerox nagyjából húsz éve fejlesztette ki ezt a technológiát, azon félelmek miatt, hogy színes nyomtatóikkal bankjegyeket lehet majd hamisítani. Azóta számos vállalat rendszerbe állította ezt az eljárást.

ADATMENTŐkések

Információ-újgazdagok

Talán furcsán hangzik, de aki kényes információkat akar papírra vetni, az írja meg szabadkézzel, vagy használjon hagyományos írógépet, melyek a számítógépek korában már teljesen elavultak. Ezek nagy része nem beazonosítható (jelenleg csak olyan írógépekről vannak írásminták elraktározva a bűnügyi nyilvántartásokban, amelyekkel bűncselekményt követtek el), így nyugodtan lehet velük dolgozni. Igaz, hogy sokkal időigényesebb, de biztonságosabb.

Ennek az az oka, hogy minden betű, szó és mondat, amelyet számítógéppel írtunk, rákerül a komputer merevlemezeire, és ha már rajta van, azt onnan el is lehet olvasni. A köztudatban az van, hogy amikor megnyomják a „delete vagy a cancel" billentyűt, akkor letörlődik az összes információ a gépről, de nem: a merevlemezen nullák és egyesek formájában rajta marad, majd felülíródik, rétegről rétegre. Ezért veszélyes a cégek számára, amikor „üresnek" hitt használt gépeket értékesítenek vagy dobnak ki a szemétbe.

Vannak cégek, amelyek adatmentéssel, adatbányászattal, adathelyreállítással foglalkoznak. Ezeknek szó szerint aranybánya egy használt vagy sérült, mások számára értéktelen merevlemez. Az általuk alkalmazott és kifejlesztett eljárásokkal helyre tudják állítani a sérült lemezt, és a teljes tartalmát vissza tudják fejteni, így olyan információk birtokába kerülhetnek, amelyek esetleg másoknak kompromittálóak, és visszaélésekre adhat lehetőséget a

későbbiekben. Az ilyen cégek a legjobban fizetett vállalatok közé tartoznak, mivel főleg a kormányoknak és azok védelmi és irányító szerveinek dolgoznak (nemzetvédelmi és biztonsági szolgálatok, adó- és pénzügyi ellenőrző hivatalok). Tevékenységük szigorúan titkos körülmények között folyik, ezért az ellenőrzésük is.

A profi szakembereiket nagyon jól megfizetik. Nehéz ilyen cégekhez bejutni, de onnan elmenni is. A legszigorúbb ellenőrzéseken kell átesniük, mielőtt dolgozni kezdenek. Jómagam szkeptikus vagyok az ilyen munkát végzőkkel szemben, mert egyrészt a mindenkori államvezetés és apparátus szolgálatában állnak (innen kapják a legnagyobb megrendeléseket), így az általuk megszerzett, esetenként terhelő információkat közvetlenül átadhatják a megfelelő szerveknek, másrészt ilyen szinten nem hiszek a titoktartásban. Kormányok jönnek, kormányok mennek, de ők megingathatatlanul, állhatatosan végzik a munkájukat. Érdemes átgondolni!

Én biztos, hogy nem bíznám rájuk a számítógépem merevlemezét, inkább fejszével apró darabokra zúznám (ez a legbiztonságosabb módja az információ megsemmisítésének). Őszintén! Mi a biztosíték arra, hogy nem készítenek az adataimról másolatot, vagy hogy valamikor nem élnek vissza az általuk előbányászott és eltárolt információkkal? Ők is emberből vannak!

Egy terhelő bizonyítékot úgy is fel lehet használni (erre megvannak a megfelelő módszerek), hogy a gyanúsított még véletlenül sem jön rá arra, honnan ered az információ. Az ilyen vállalatok vezetői, tulajdonosai „köztiszteletben álló" személyek, akik nagy szolgálatot tettek már eddig is a kormánykoröknek. A szakma csúcsán trónolnak,

és a pozíciójuk stabil. Az sem véletlen, hogy a világon elenyészően kevés ilyen cég található. Mivel kevesen vannak, így könnyebben lehet ellenőrizni a tevékenységüket. Mint jó „csatlósok", állandó készenlétben állnak, és számukra az országhatárok és a kontinensek sem jelentenek akadályt. Tevékenységük nagyon fontos, de egyben iszonyúan veszélyes is! Ránk nézve...

RFIDeológia

Rádiófrekvenciás eszmerendszer

A MARC egy olyan személyazonosítási chipkártya, amelyet az amerikai hadsereg részére fejlesztettek ki, a katonai személyzet nyomon követésére és ellenőrzésére világszerte. Különböző katonai egységekben több ezer katonán próbálták ki, de millióknak szándékoznak kiosztani. A kártyán egy mágnescsík és egy mikrochip is van. Tulajdonosa személyes és egészségügyi adatait tárolja. A kártyát azonosításra, orvosi ellátásra és más célokra használják. Azt állítják, hogy a MARC a Multi-technology Automated Reader Card (többtechnológiás, automatikusan leolvasható kártya) rövidítése. De ugyanúgy hangzik, mint a mark (magyarul: bélyeg), a Fenevad bélyege a Jelenések könyvéből. Néhány bátor katona visszautasította a kártya használatát, vállalva a következményeket, mert ráébredtek annak profetikus jelentőségére.

A beültethető mikrochip egy olyan készülék, amely rizsszem nagyságú üvegtokba zárt elektromágneses tekercsből és egy mikrochipből áll. Jelenleg állatokba ültetik be, és fejlettebb utódait emberi alanyokon próbálják ki világszerte. Előfordulhat, hogy a beültethető mikrochip nemsokára felváltja a bankkártyákat, a kártya formátumú személyi igazolványt, és a többi kártyát. A bőr alá betett mikrochip lehetővé fogja tenni befogadójának a megfigyelését, és valószínűleg agykontrollját is.

A legegyszerűbb beültethető mikrochip egy miniatűr, áramforrás nélküli passzív válaszjeladó (transzponder). A benne levő chip egy állandó, egyedi azonosítási számot

tárol, amit el lehet olvasni, de nem lehet megváltoztatni, tehát ez a készülék csak olvasható (read-only). Külső olvasók vagy szkennerek kisfrekvenciás rádióhullámokkal működésbe hozzák a válaszjeladót, amely a tárolt szám kisugárzásával válaszol. A készüléket beültethető transzpondernek vagy RFID címkének is hívják. Az RFID a Radio Frequency Identification (rádiófrekvenciás azonosítás) rövidítése.

2005-ben az RFID a kísérleti laboratóriumból kikerül végre a kereskedelmi forgalomba. A nagy kereskedelmi láncok, a nemzetvédelem beszállítói, az autógyártók és egyéb szereplők – amelyek mindegyike megköveteli beszállítóitól az RFID használatát – együttes befolyása szinte a nulláról kezdve óriási növekedést indít el az RFID alkalmazásában. Az év végére több milliárd RFID azonosítót értékesítenek és használnak majd.

Az RFID nem pusztán a vonalkódot váltja föl: egy olyan technológiát jelent, amely hozzájárulhat a hulladék újrahasznosításához, a lopások számának csökkentéséhez, a raktárkészletek kezeléséhez, a logisztika gördülékenyebbé tételéhez, vagy akár a termelékenység növeléséhez. Ezeknek az RFID adatoknak az összegyűjtése, egyeztetése és bemutatása hamarosan tekintélyes méretű iparággá fejlődik, amelyből az informatikai vállalatok szerzik meg a bevételek oroszlánrészét.

Az RFID olvasók és egyéb hardverek szintén nyereséges piacot teremtenek majd. Az RFID alkalmazásokat használják majd az egészségügyben (a betegek megfigyelésére), az építőiparban (projektek irányítására és a felszerelések kezelésére), sőt még a közlekedésben is (a repülőtereken az utasok és a poggyászok nyomon követésére).

A Sagem a közelmúltban írt alá egy 8 éves szerződést a

Northrop Grumman Information Technology-val biometriai azonosító technológia szállítására, melyet egy olyan számítógépes rendszer frissítéséhez használnak majd, ami több mint 50 rendőrséget köt össze az Egyesült Királyságban. A Sagem által szállított technológiát a Northop Grumman IT cég integrálja Anglia és Wales jelenlegi automatikus ujjlenyomat-azonosító rendszeréhez (Automatic Fingerprint Identification System), valamint a skót rendőrség által használt AFIS rendszerhez. A jelenlegi szolgáltatások azt teszik lehetővé a rendőrségeknek, hogy a nemzeti adatbázisukban keressék az ujjlenyomatokat és a bűntények helyszínén rögzített bűnjeleket. A későbbiekben ezek az országos rendszerek egy globális azonosító rendszerbe lesznek beintegrálva, így a bűnözők bárhol is hagynak maguk után értékelhető ujj-, tenyér- vagy más bőrlenyomatot, a rendszer pillanatokon belül be fogja azonosítani.

Az új rendszer viszont, melyet IDENT1-nek hívnak, biztosítja annak lehetőségét, hogy az ujjlenyomatokat egy olyan összevont adatbázisban keressék, amely több mint 6 millió tenyérlenyomatot tartalmaz. Az IDENT1 egyik első fejlesztése, melyhez a Sagem nagymértékben hozzájárul, egy nemzeti tenyérlenyomat-kereső szolgáltatás létrehozása lesz. Ennek a szolgáltatásnak a segítségével lehetővé válik, hogy a letartóztatottaktól már amúgy is rutinszerűen levett tenyérlenyomatokra is ugyanolyan keresést lehessen végrehajtani, mint az ujjlenyomatok esetében. A tenyérlenyomatok keresése jelentős hatással lesz a bűnügyek feltárására, mivel az Egyesült Királyságban a bűntények helyszínén feltárt bűnjelek közel 20%-a tenyérlenyomat.

A további fejlesztések tartalmaznak majd mobil ujjlenyomat-ellenőrző berendezéseket, arcrögzítést és videós azonosítást. „Az Egyesült Királyság létrehozott egy szabványt, ami a rendőrség azonosítási technológiájára vonatkozik, és lehetővé teszi a teljes körű keresést és összehasonlítást. Ez a szerződés biztosítja számunkra, hogy folytassuk ezt a munkát, és a rendőrséget további olyan szolgáltatásokkal lássuk el, amelyek segítségével harcolhatnak a modern, kifinomult és mobil bűnözők ellen" – állítja Dr. Fred Preston, az Egyesült Királyság Rendőrsége IT szervezetének (PITO) azonosításokért felelős igazgatója.

Jean-Paul Jainsky, a Sagem biztonságtechnikai üzletágának igazgatója a következőt nyilatkozta: „Úgy tekintjük ezt a megállapodást, mint egy kitűnő kapcsolatot két cég között, és meggyőződésünk, hogy a SAGEM egyedülálló és jól megalapozott szakértelme a nagy biometriai azonosító rendszerek tervezésében és telepítésében gyorsítani fogja az Egyesült Királyság rendőrségeinek fejlesztését. Ezzel a sikerrel a SAGEM újra megerősíti vezető pozícióját a biometriai rendszerek gyorsan növekvő piacán."

Az illegális szervkereskedelmet a holttestekbe ültetett elektronikus azonosítóval akarja megelőzni egy kaliforniai egyetem. Az ún. „RFID tag"-ek kisméretű címkék, amelyek chipen tárolják az információt, az antennával felszerelt RFID-vevők pedig az elektromágnesesség elvén képesek olvasni a címkéken lévő adatokat. Léteznek passzív és aktív RFID címkék is: az előbbiek kisebb hatótávolságúak, viszont nem igényelnek külön áramforrást. A rádiófrekvenciás címkéket ma is széles körben használják, például könyvtári könyvek, a repülőtéren feladott csomagok nyomon követésére, vagy a boltokban lopásgátlásra.

Vonalkóddal vagy rádiófrekvenciás azonosító chipekkel látnák el az Egyesült Államokban azokat a holttesteket, amelyeket eredeti „tulajdonosuk" tudományos célok-

ra ajánlott fel még életében. A Kaliforniai Egyetem (UCLA) kutatói nemrégiben azért javasolták a hullák nyomon követésére alkalmas módszert, mert a fogadó intézmények sokszor nem kellő tisztelettel bánnak a holttestekkel, illetve a belőlük származó szervekkel, és arra is több példa volt már, hogy a jó szándékú – ingyen adakozó – donoroktól származó testrészek szervtőzsdéken tűntek fel. És bár az Egyesült Államokban szövetségi törvények tiltják a szerv- és szövetkereskedelmet, a feketepiacon több tízezer dollárért cserélnek gazdát a halottakból kioperált testrészek.

2004-ben a UCLA kénytelen volt felfüggeszteni „Willed Body" (kb. „testált test") projektjét, miután a program igazgatója és egy munkatársa illegális szervkereskedelem gyanújába keveredett. A kilencvenes évek végén egy másik program igazgatóját rúgták ki, mert állítólag emberi gerinceket adott el egy arizonai kórháznak, és az intézet nem tudott elszámolni több száz holttesttel. A donorok hozzátartozói 1996-ban be is perelték az egyetemet, ahol állításuk szerint a holttesteket állati tetemekkel és elhalt magzatokkal együtt hamvasztották el, és a maradványokat a szemétbe dobták.

Az egyetem által most fontolóra vett rádiófrekvenciás azonosítók (RFID címkék) egy, a közfelháborodás hatására már korábban megkezdett intézkedéssorozatba illeszkednének; amelynek részeként a UCLA javított a donornyilvántartó rendszeren, illetve elektronikus zárakkal és megfigyelőkamerákkal szerelte fel az egyetem különböző helyiségeit. Az Egyesült Államokban évente több ezer holttestet adományoznak szövetbankoknak és egészségügyi intézményeknek.

A testeket nem csak szervátültetésre használják, de biztonsági felszereléseket, így bukósisakokat is tesztelnek rajtuk. Az ötvenes évek végén holttesteket kezdtek használni az autókon végzett töréstesztek során is, és bár abban az időben készültek már tesztbábuk is, Amerikán kívül több országban, elsősorban Franciaországban, Németországban és Japánban ma is használnak hullákat a balesetszimulációkhoz.

A UCLA javaslata még részletes kidolgozásra vár, így az sem dőlt el, egyszerű vonalkóddal vagy modernebb, egyedi azonosításra alkalmas és nagyobb távolságból is leolvasható chipekkel követik majd a holttestek útját. Azt viszont a terv kidolgozói valószínűnek tartják, hogy a hullákból eltávolított szerveket el kell majd látni az elektronikus azonosítókkal. A Cisco és az Európai RFID Központ bejelentette, hogy a Cisco is csatlakozik a Központ kezdeményezéséhez annak érdekében, hogy elősegítsék az RFID-n alapuló üzleti alkalmazások európai elterjedését. A központ célja, hogy élő bemutatók, képzések, rendezvények és pártatlan tanácsadás útján demonstrálja a rádiófrekvenciás azonosítási alkalmazások előnyeit az európai vállalkozások számára.

A Heathrow repülőtér közelében, Bracknellben található központ számos technológiai partner, köztük a Microsoft, az Intel és a Cable & Wireless, valamint a brit kereskedelmi és ipari minisztérium támogatásával jött létre. A rádiófrekvenciás azonosítás bevezetése és használata sokak érdeke, a kutatószervezetben több ismert multinacionális cég is részt vesz. A szabványok kidolgozásában, az alkalmazható eszközök, címkék, leolvasók technológiájának fejlesztésében, illetve a költségszintek csökkentésében olyan cégek dolgoznak együtt, mint a Coca Cola, a Gillette, a Johnson & Johnson és az Unilever.

Amíg a gyártószalagról a boltok polcaira kerül az áru,

hosszú utat tesz meg: csomagolják, tárolják, viszonteladókhoz szállítják, majd onnan eljuttatják a boltokba. Ezen az úton az áruk egy részének óhatatlanul nyoma vész. Becslések szerint a leltári pontatlanság, a raktározás során félreszámolt tételek, a szállítás hiányossága vagy gondatlansága, valamint a lopások miatt csak az Egyesült Államokban évente 33 milliárd dollár veszteséget kénytelenek elkönyvelni a kiskereskedelemben – ami további 38 milliárd dollárnyi kárt okoz azáltal, hogy a vásárlók nem találják a boltok polcain az általuk keresett terméket.

Joggal merült fel hát az igény egy olyan megoldás iránt, amellyel az ellátási lánc teljes szélességben könnyen átláthatóvá, ellenőrizhetővé tehető, amivel a hibák és hiányosságok gyorsan kiszűrhetők, s így a károk minimálisra csökkenthetők. Erre a problémára az elektronikus termékkódot hordozó rádiófrekvenciás azonosító címke kínál megoldást.

A rádiófrekvenciás azonosító címke egy 96 bit információ tárolására képes, 0,3 mm méretű mikrochipből és egy antennából áll. Ha a mikrochip egy erre a célra kifejlesztett, elektromágneses mezővel körülvett leolvasóberendezés közelébe kerül, rádióhullámokon keresztül automatikusan kommunikálni kezd vele, és elküldi a rajta tárolt információt: az elektronikus termékkódot képező numerikus adatsort.

A leolvasóberendezés ezredmásodpercek alatt fogadja az információt, majd továbbítja egy szerverre, ahonnan az adatokat elektronikus úton az arra jogosultak akár az internet segítségével elérhetik. Az elektronikus termékkód előnye a vonalkódhoz képest, hogy a használatával minden egyes termék egyedi módon azonosítható, és az interneten tárolt adatokkal összekapcsolható, így az egy-

egy termékhez egyedi módon hozzárendelhető információk száma végtelen.

Amíg a vonalkód csak az árucikk megnevezésére, árára és gyártójára vonatkozó – maximum 12–14 bit méretű – információt tud tárolni, addig az elektronikus kód alapján többek között megállapítható, hogy hol, mikor és ki gyártotta az adott terméket, milyen úton jutott a bolt polcaira, a szállítás során megfelelő módon kezelték-e, és minőségét meddig őrzi meg.

Az elektronikus kód további előnye a vonalkóddal szemben, hogy leolvasása automatikusan, emberi közbeavatkozás nélkül történik: elég, ha a felcímkézett terméket (akár több ezer darabot dobozba csomagolva egyszerre) eltolják a leolvasóberendezés mellett. A 96 bites kód 268 millió cégnek biztosíthat egyedi azonosítót, cégenként 16 millió tárgykategóriával, kategóriánként 68 milliárd szériaszámmal.

Az RFID technológia üzleti életben való alkalmazása ma már nem távoli jövő, hanem kézzelfogható valóság. Bevezetésétől a Gillette éves bevételének 3-5%-os emelkedését várja, a Procter & Gamble pedig az ellátási lánc működtetésével kapcsolatos költségeinek 1,5 milliárd dolláros csökkenésére számít. A Wal-Mart, a világ legnagyobb áruházlánca 2005. január 1-jétől megköveteli száz legnagyobb beszállítójától, hogy termékeit rádiófrekvenciás azonosító címkével lássák el.

A Delta Airlines egy pilot teszt keretében 40 ezer utasának poggyászát címkézi fel, a Goodyear szintén a technológia bevezetését tervezi. Az Egyesült Államokban 2003-ban 91,5 millió dollárt költöttek RFID technológiára a kiskereskedelmi ellátóláncban; egy statisztikai előrejelzés szerint ez a szám 2008-ra 1,3 milliárd dollárra nő.

Alkalmazási területei szinte határtalanok: alkalmas lehet

a postai szolgáltatások minőségének emelésére, a gyógyszerhamisítás megakadályozására, az élelmiszerek előállításának és biztonságos szállításának ellenőrzésére, sőt a pénzhamisítás és a pénzmosás meggátolására is. E mostanában rendkívül divatos témáról folyamatosan jelennek meg a kutatásokról szóló hírek, s ezek rendszerint mindent elsöprő növekedést prognosztizálnak.

A svájci–német Soreon Research piackutató cég előrejelzése szerint az RFID-piac Európában 400 millió euróról 2,5 milliárd euróra fog növekedni az elkövetkező négy évben. A piac forgalmának egyötöde a szolgáltatók zsebébe vándorolna; ennek az összegnek több mint háromnegyedét a folyamatos árcsökkenés ellenére is az áramkörökből származó bevétel tenné ki. 2008-ig minden huszadik termékre kerül azonosító címke – vélekedett az elemző cég.

A szakértők a Metro Group, a Wal-Mart és a Tesco kereskedőházakat tartják az RFID-őrület előkészítőinek. A Soreon szerint a nagykereskedelmi cégek számíthatnak az érintésmentes azonosításba befektetett összeg legnagyobb mértékű megtérülésére, mivel meg tudják fizetni az okos címkék árát beszállítóiknak. A piackutató cég a gyártóknak azonban azt javasolja, hogy késleltessék az RFID bevezetését: a tanulmány szerint a várakozás minden egyes hónapjával egyre alacsonyabb lesz a címkék ára, így csökkenthető a beruházás költsége. A Metro és a Wal-Mart ugyanakkor már kötelezte a legfontosabb beszállítóit, hogy áruikat még ebben az évben RFID címkékkel lássák el.

A nagy informatikai világcégek – a Sun Microsystems, az IBM, a HP – egymástól függetlenül, nagy erővel dolgoznak RFID-fejlesztéseken. A HP két RFID-partnerségi programot indított, s a következő öt évben 150 millió dolláros kutatási alapból fedezi az RFID-fejlesztéseket. Az IBM 5 év alatt 250 millió dollárt akar az érzékelők és más, az RFID-rendszereken használt eszközök fejlesztésére. Mint láthatják, ennek az őrült versenynek az a végső célja, hogy a jövőben ne legyen olyan tárgy vagy élőlény a világon, amelyet nem lehet beazonosítani valamilyen módszerrel.

ÚTLEVÉLetfogytig

Az utolsó útlevél

Az Európai Unió hivatalos lapjában is megjelent, és ezzel életbe lépett az Európai Tanácsnak az a 2004 decemberi rendelete, amely szerint a tagállamoknak legkésőbb 2006 júniusáig – tehát a korábbi hírekkel szemben egy évvel korábban – be kell vezetniük a biometrikus adatokat tartalmazó útlevelet. Bár az Európai Parlamentben heves vita folyt erről, a liberálisok és a Zöldek alulmaradtak – a képviselők többsége szabad utat adott a mintegy 450 milliónyi uniós polgárt érintő változásnak.

Ezt a drágább okmányt eleinte csak azoknak kell kiváltaniuk, akik az Egyesült Államokba utaznak, az uniós országokban ugyanis (érvényességi idejük lejártáig) elfogadják a régi útlevelet is. Az amerikai hatóságok így is készítenek majd rólunk digitális felvételt, hiszen ez náluk minden vízumköteles ország polgárára érvényes szabály. Az uniós országoknak a több tízmilliárd eurós beruházást igénylő új rendszer bevezetéséből egyelőre nem sok hasznuk lesz.

Az új úti okmányok bevezetésére a hamisítók dolgának megnehezítésére van szükség, továbbá csak így biztosítható, hogy az európai uniós országok állampolgárai 2005 ősze után is vízummentesen utazhassanak az Egyesült Államokba. Az egyetértés ebben a kérdésben itt már ki is merül. Ami biztos még, hogy az új útlevelek készítési költségeit is a polgároknak kell fedezniük. Jelenleg egy német útlevél elkészítése 26 euróba kerül, a tervek szerint azonban – és ettől tart több európai politikai párt is, így például a németországi FDP és a Zöldek – az új biometriai okmányok gyártási költsége a mostani díj többszöröse is lehet majd.

Érthető tehát, hogy egyre több európai uniós államban egyre idegesebben teszik fel a kérdést a polgárok: konkrétan mennyibe is fog kerülni az új úti okmány?

Csak olaj volt a tűzre Silke Stokarnak, a 90-es Szövetség/Zöldek tömörülés belpolitikai szóvivőjének tavaly december elején tett nyilatkozata, miszerint a biometriai azonosítókkal ellátott útlevelek ára elérheti majd akár a 130 eurót is. Stokar úgy véli: abszurd lenne ezeket a költségeket az állampolgárokra áthárítani, és ez az összeg elfogadhatatlan. Egyes politikusok szerint még ennél is magasabb költségvállalásra kerülhet sor.

A témához kötődő híreket elemezve láthatjuk, hogy az Európai Parlament tavaly decemberben, költségbecslés nélkül fogadta el a biometriai igazolványok bevezetéséről szóló javaslatot. A német parlament technikai következménybecslő irodája szerint csak Németország számára ez 669 millió euró egyszeri, és akár 610 millió eurós éves költséget jelent. Ügyes elgondolás! Fizessünk azért, hogy még jobban, könnyebben és gyorsabban meg tudjanak minket figyelni. Tudniillik, ha egy ilyen útlevél van a birtokunkban, a műholdak segítségével be lehet azonosítani a tényleges tartózkodási helyünket.

Az Európai Tanács határozata értelmében minden igazolványnak két ismertetőjegyet kell tartalmaznia: ujjlenyomatot és arckarakterisztikai lenyomatot. A korábban szintén szóba került íriszazonosítást elvetették, a későbbi lehetséges nemzetközi szabadalmi viták elkerülésére. Az adatokat az okmányokban chipekben rögzítenék. Az alkalmazandó személyazonosító módszerek tévedhetetlen-

sége azonban még korántsem bizonyított. Azok a kérdések is megválaszolatlanok, hogy hová, milyen központ(ok)ba kerülnek az így rögzített személyes adatok; ki(k) és milyen mélységig férhet(nek) ezekhez hozzá; mi a garancia arra, hogy a kormányok vagy a hatóságok nem élnek vissza ezekkel az információkkal.

Ezek után nem lehet csodálkozni azon, ha valakinek az az érzése kezdene kialakulni, hogy – kis túlzással – egy digitális ketrecre hasonlít lassan az Európai Unió, és az egész világ. Úgy tűnik, mintha egyik ország minisztériumai és szakhatóságai sem akarnák pontosan felvilágosítani az állampolgárokat, hogy miről is van szó; hogy az amerikai terrorellenes nyomáson kívül miért van szükség a biometriai adatok rögzítésére. MIÉRT? A rendelet szerint az egységes európai útlevél bordó színű lesz, az adatoldal előre kerül, és a borítójában mikrochipet kell elhelyezni. Ez jövő nyártól egyelőre csak a tulajdonos képmását tartalmazza elektronikus formában, 2008 végéig azonban az ujjnyomatot is hasonlóképpen rögzíteni kell. A sietség oka az, hogy az USA a jövő ősztől már csak az elektronikus adathordozójú útlevelet fogadja el. A Brüsszelben meghozott döntés az unió összes tagországára érvényes. Az útlevelek lecserélése ugyan több milliárd euróba kerül, azonban a biztonság minden pénzt megér. A bordó útlevelek látszólag csak színükben különböznek a jelenlegitől. Holott a látszat csal. Az első, megvastagított oldalban ugyanis egy kis chip tárolja majd mindannyiunk egyénre jellemző tulajdonságait.

Néhány kormány már döntött, annak ellenére, hogy az útlevelek cseréje több milliárd euróba fog kerülni. A biztonság nem állítható arányba a költségekkel, állítják a szakemberek. De semmi nem bizonyítja, hogy a szabadságjogok korlátozása arányban áll a biztonság növekedésével. Ez egy rossz asszociáció. Amikor az ujjlenyomat használatba került, gyakorlatilag a bűnözők megkülönböztetésére szolgált. A mostani terv ellenben azt jelenti, hogy az összes uniós állampolgár rabosítására kerül sor. Útlevélhez legkorábban 3 év múlva vesznek ujjlenyomatot, akiknek azonban tovább érvényes útlevelük van, azoktól még később.

Annak ellenére, hogy a schengeni egyezmény szerinti szabad határok elve még vitatott, a felkészülés már javában folyik az EU-hoz újonnan csatlakozott tagországokban. A határok, határátkelőhelyek felkészítése a schengeni követelmények teljesítésére komoly modernizációs feladatokat foglal magában, melyhez – többek között – a Schengeni-alap nyújt támogatást a csatlakozó tagországoknak.

A magyar biztonságtechnológiai iparág élen jár az előírások teljesítéséhez szükséges fejlesztések és gyakorlati megvalósítások terén. A schengeni térség közös adat- és információs rendszer (Schengeni Információs Rendszer – angolul SIS) működtetését igényli, amihez az új tagok csatlakozása elengedhetetlen. Ennek az információs rendszernek a jövőben képesnek kell lennie összetett, különleges adatok kezelésére is. A térség biztonságának fenntartását szolgálják majd az információs technológia legújabb vívmányai is. A személyek azonosításában jelentős szerepet kapnak az útlevélbe épített RFID-chipek, melyek felismerését a magyar fejlesztésű „Passport Reader" okmányolvasó készülékek már biztosítják.

Egy másik várható követelmény a biometrikus adatok ellenőrzése. Ennek egyik lehetséges módja az arcfelismerésre alkalmas technológia alkalmazása – erre is van már

felhasználható magyar megoldás: „FaceIdent". A schengeni térséghez a közeljövőben csatlakozó országok érdekeltek abban, hogy a feltételek teljesítésében együttműködjenek, segítsék egymást.

A környező országokban megindult készülődésben mind az okmányolvasás, mind pedig a rendszámfelismerés területén jelentős szerepet vállal a magyar biztonságtechnológia. A történelemből ismert magyar tudósok hírnevét öregbítik ezek a technológiai találmányok és fejlesztések is. De ha mélyebben belegondolnának abba, hogy milyen célt is szolgálnak ezek a csúcstechnológiák, akkor nem lennének ilyen büszkék rá.

Szlovákiában már évek óta bizonyítanak a magyar okmányolvasók, és a közelmúltban kiértékelt tenderen minden valószínűség szerint ismét a magyar megoldást választották: a CARMEN rendszám-azonosítót. Lengyelországban a próbarendszerek tesztelése és kísérleti üzemeltetése már sikeresen befejeződött, így itt is várható a magyar technológia térhódítása. A határok korszerűsítésében az EU-hoz a közelmúltban csatlakozott országok szomszédjai is érdekeltek. Horvátország belügyminisztériuma a magyar szakembereket vonta be a felkészüléssel kapcsolatos tervezésbe. Ukrajna és Bulgária határain már évek óta használják a magyarok által fejlesztett technológiát, illetve Románia is érdeklődést mutat a magyar termékek iránt, határátkelőinek informatikai korszerűsítéséhez. A fenti tények alapján kijelenthetjük, hogy a teljes új schengeni határ meghatározó hányadán növeli majd a „biztonságot" a magyar „sikertechnológia".

A rendeletekben foglaltakat a tagállamoknak végre kell hajtaniuk, ezért a nemzeti vízum- és okmánybizottságok már vizsgálják, hogy milyen intézkedésekre van szükség.

Az biztos, hogy gyakorlatilag egy vadonatúj okmányt kell előállítani, és ez az okmánycsere az adófizetők zsebéből veszi ki majd az eurómilliárdokat. Az adatvédelmi biztosok és mások is tiltakoznak a biometrikus adatok rögzítése ellen. A kormányok ezekre reagálva hangsúlyozzák: az unióban nem lesz egységes adatbázis. Ez a kijelentés nevetséges, mivel már most is van! Azt állítják, hogy minden információt a mikrochippel ellátott vízumban tárolnak, és külön tagállami nyilvántartások működnek majd. A polgároknak ugyanakkor lehetőséget kell biztosítani arra, hogy okmányuk tényleges adattartalmát (a chipben rögzített információt is) bármikor ellenőrizhessék (erre szerintem nem sok alkalmunk lesz).

Én még nem tapasztaltam olyat, hogy egy bankkártya használatánál az olvasó LCD kijelzőjét felém fordították volna egy bankban, hogy elolvashassam a rólam tárolt információkat, mert azok banktitoknak minősülnek. Még nekem, a tulajdonosnak is?! A színfalak mögé mi, egyszerű állampolgárok nem láthatunk, a kormány eddig is azt csinált az adatainkkal, amit akart.

MIKROCHIPParág

Kicsi a chip, de okos

A mikrochip-iparág félelmetes gyorsasággal fejlődik. Pár évvel ezelőtt azt sem tudtuk, hogy mi az a nanotechnológia, most meg már nanochipekről hallani, amelyek teljesen átírják az informatika, a kommunikáció történelmének lapjait.

Írható-olvasható (read-write) mikrochipek is léteznek, melyekben a tárolt információt meg lehet távolról változtatni. A fejlettebb beültethető mikrochipek nem csak írhatók-olvashatók, hanem egy azonosító rádiójelet is kibocsátanak, melyet nyomon lehet követni, és azáltal a megcímkézett személy vagy állat folyamatosan megfigyelhető. Ezekben a készülékekben áramforrás is van.

A legújabb beültethető mikrochipekben számos mikroprocesszor van, és egy miniatűr digitális adó-vevő. A befogadó személy izmainak mozgása biztosítja elektromechanikusan az áramot. Ezek a készülékek évekig működőképesek maradhatnak a testben. Tulajdonképpen apró számítógépek, melyek adatokat is tudnak venni, illetve sugározni távoli érzékelőkhöz, és folyamatosan nyomon követhetők a globális helyzetmeghatározó műholdak (GPS) segítségével.

Az a számítógép-teljesítmény, amelyhez egykor egy egész épületre szükség volt, most beültethető egy ember karjába.

Az emberek általában nem tudják, hogy bizonyos tárgyakba mikrochipek vannak beépítve, és ha tudnák sem biztos, hogy zavarná őket, mert manapság nagyon sok

termékben található elektronika. Élőlényekbe, főleg emberekbe ültetni elektronikus szerkezeteket már egészen más.

Visszataszítónak tűnik, és nem csak a keresztények számára, hanem az összes jóérzésű, normálisan gondolkodó embernek. Ezért az embereket e módszer elfogadására agymossák. Megvan az engedély! Eztán mikrochipeket is lehet beültetni az emberi testbe – állítólag orvosi célokra –, de máris sokan aggodalmaskodnak, vajon nem afféle mindent ellenőrző rendszer kiépítéséről van-e szó, és sokan tiltakoznak, a személyiségi jogok sárba tiprását emlegetve.

Egy floridai vállalat rukkolt elő az ötlettel és magával a termékkel is. A VeryChip nevű kis szerkezet akkora, mint egy rizsszem, a bőr alá ültethető be. Észrevétlen, és egészségügyi, orvosi információkat továbbít arról az emberről, akibe beültetik. Készítői szerint a láthatatlan mikrochip akár a páciens életét is megmentheti. A bőr alá helyezett kis azonosító rádióhullámokkal kommunikál, és bárhonnan figyelemmel kísérhető.

Az amerikai élelmiszer- és gyógyszer-engedélyező hivatal a napokban rányomta a pecsétet a kérelemre. A VeryChip tehát mostantól beültethető emberbe. De meg sem száradt a pecsét az engedélyen, különféle szervezetek és hivatalok máris a mikrochip más jellegű alkalmazását is latolgatják. És mivel az Egyesült Államokban mostanság a biztonságot mindennél előbbre valónak tartják, olyan tervekről szivárognak ki hírek, hogy katonai bázisokon, atomerőművekben, sőt, szövetségi kormányzati hivatalokban is alkalmaznák majd. Magyarán az ott dolgozóknak – akarják-e vagy sem – beültetik a bőre alá a mikrochipet, rátelepítve a személyes adatokat, és így nemcsak hogy

belépőigazolvány, belépőazonosító nem kell majd, hanem az illető mozgása állandóan szemmel tartható.

A módszert, mármint a chipbeültetést állítólag Japánban már kísérleti jelleggel ugyan, de alkalmazzák, elsősorban iskolákban, a gyerekek megfigyelésére. Nos, éppen ez a megfigyelés aggaszt egyes amerikai emberi jogi szervezeteket. Az amerikai Polgári Szabadságjogok Uniója nevű szervezet már arra szólította fel a virginiai hatóságokat, hogy a jogosítványokba ne tegyenek be ilyen chipeket. Ezek révén ugyanis könnyen beazonosíthatóak lesznek a politikai megmozdulásokon vagy a tiltakozó menetekben részt vevők, vagy akár az Államokba érkező turisták, vagy a valamilyen okból megfigyelendők. Elektronikusan figyelik majd a világot? – kérdezi a szervezet, és azzal érvel, hogy mindennek a politikai következményei beláthatatlanok.

Az emberbe ültethető mikrochipek jövőbeni felhasználásának víziója, bizony, riasztó lehet, talán még tudományos-fantasztikumnak is tűnhet. Olyasminek, mint jó néhány évvel ezelőtt a híres-hírhedt Kóma című film sztorija, ami arról szólt, hogy kómába esett emberekből kioperálják az egészséges szerveket, és feketekereskedelemben forgalmazzák, szervátültetésre váró gazdagoknak adják el őket. Sőt, egészséges embereket rabolnak el, mesterségesen kómába ejtik őket, hogy kioperálják szervezetükből az egészséges szerveket.

Amikor sok-sok évvel ezelőtt vetítették a filmet, megborzongtunk, de aztán legyintettünk: ugyan, ez csak film, ez csak kitaláció, ilyen a valóságban úgysem történhet meg. Nos, néhány év óta az úgynevezett harmadik világ egyik legtragikusabb gondja a szervkereskedelem. De nehogy így járjon az emberiség a bőr alá ültethető chipekkel

is! A „chipelést" úgy reklámozzák, mint az elveszett állatok megtalálásának az egyik legjobb módját. Az állatorvos egy különleges fecskendővel ülteti be a mikrochipet az állat bőre alá. Ennek a passzív válaszjeladónak nincs szüksége tápegységre, ezért évtizedekig működhet. A chip egy egyedi azonosítási számot tartalmaz, amelynek alapján az országos háziállat-adatbázisból kikereshető a tulajdonos neve, címe és telefonszáma. Az állatmenhelyeken a talált állatokat kézi szkennerekkel „leolvassák", és visszajuttatják gazdáiknak.

Ez a technológia elsősorban a nyugati országokban használatos kutyák, macskák, madarak, gyíkok és más háziállatok esetén. Lovakba, haszonállatokba, vadállatokba, sőt még halakba is ültetnek mikrochipeket, hogy műholdak segítségével nyomon követhessék őket, és megfigyelhessék vándorlásukat. A Brit Honvédelmi Minisztérium bevezette a mikrochipes azonosítási rendszert az összes brit katonai szolgálatot teljesítő állat számára világszerte. Amerikában például 1999. július 1-je óta kötelező az újszülött kiskutyák mikrochipelése!

1997 telén az amerikai híradások svábbogarakon végzett agykontroll-kísérletekről számoltak be. Ezeknek a high-tech svábbogaraknak a testébe beültettek egy minielektródás hátizsákot, melynek következtében az összes mozdulatuk távirányíthatóvá vált. Hogyha az történne, amit a kutatók akarnak, nem telne sok időbe, és hasonlóan felszerelt rovarok mászkálnának földrengés után a kőtörmelékek között, áldozatok után keresgélve, vagy ajtók alatt bújnának át kémkedési kiküldetéseken.

Bár itt kimondottan agykontroll-kísérletről van szó, minket azzal nyugtatgatnak, hogy a mi érdekünkben történik. Amennyiben valakibe beültetnek egy miniatűr digitális

adó-vevőt tartalmazó mikrochipet, az a személy a nap 24 órájában nyomon követhetővé válik az egész világon műholdak, földi érzékelők és számítógépes hálózatok segítségével. Ennek a ténynek már önmagában elegendőnek kellene lennie ahhoz, hogy ne engedjünk semmilyen szerkezetet vagy elektronikus tetoválást feltenni magunkra vagy családtagjainkra.

A számítástechnika fejlődésével a számítógépek kezdenek olyan parányiak lenni, mint egy pont, ezért nagyon apró tárgyakban is elférnek. Mivel a legtöbb embernek fogalma sincs, hogy mi folyik itt, akiknek pedig van, azok általában a „rossz fiúk", ezért nem hihetünk senkinek, aki azt bizonygatja nekünk, hogy ezek a szerkezetek ártalmatlanok.

A fő cél nem az állatok nyomon követése, hanem az emberek azonosítása, megfigyelése és irányítása. Ezt természetesen rejtegetik előlünk, nehogy felébredjünk az agymosott álmunkból. Folyamatosan felröppennek olyan hírek, kormány- és vállalati laboratóriumokban folyó, szupertitkos kísérletekről, amelyekben kiszolgáltatott emberi alanyok – többnyire halálra ítélt bűnözők – agyféltekéibe (agyába), hallószerveibe (füleibe), és testük más részeibe számítógépes chipeket, adó és vevőkészülékeket ültettek. Különböző kifogásokat találnak ki, hogy ránk kényszerítsék a mikrochipeket.

Világszerte milliók hordozhatnak mikrochipeket a testükben. A Safe Medical Devices Act (Biztonságos Orvosi Készülékek Törvénye), amely 1990-ben lépett érvénybe, megköveteli a beültetések és orvosi készülékek amerikai gyártóitól, hogy valamilyen azonosítási és nyomon követési módszert alkalmazzanak azon termékeik esetén, amelyeket emberekbe ültetnek. A befogadó személyek nyomon

követése is kötelező arra az esetre, ha működési hibák jelentkeznének. A világszerte több millió emberben levő mellbeültetések, szívritmus-szabályozók (pacemakerek), mesterséges szívbillentyűk és művégtagok mind nyomon követendők. Az egyik alkalmazott módszer a készülékek nyomon követésére az integrált mikrochipek azonos időben való beültetése, amelyek adatokat tárolnak a gyártóról, sebészről, a beültetés időpontjáról stb.

Egy amerikai flottatámaszponton őrizetben tartott több mint 50 ezer kubai és haiti menekültre mikrochipeket tartalmazó karpereceket tettek, hogy azonosíthassák és nyomon követhessék őket. Kisebb gyermekeknél a bokára tették a karperecet. Egyes menekültek megpróbálták a karpereceket levenni, ennek megakadályozására fémcsíkokat ágyaztak a pántba. Ezzel a módszerrel egy falak nélküli börtön alakítható ki, melyben az elítéltek szabadon mozoghatnak, és mégis mindig szem előtt vannak.

Versenyek megfigyeléséhez és pontos eredmények méréséhez válaszjeladót tartalmazó karpereceket tesznek a futókra és az úszókra, kerékpárversenyeknél a biciklire erősítik a válaszjeladót. Olyan javaslatok is elhangzottak, hogy a mikrochipet használják egyetemes azonosítási eszközként, és váltsák fel vele a bankkártyákat és az útleveleket is. Az emberek az üzletben úgy fizetnének, hogy kezüket, melybe a mikrochip van ültetve, elhúznák a szkennerek előtt a pénztárnál, és az összeg automatikusan levonásra kerülne a bankszámlájukról.

Az amerikai 5,629,678-es szabadalmi szám alatt, 1997. május 13-án jegyezték be hivatalosan az „embereket nyomon követő és megtaláló rendszer" alapötletét és prototípusát. Az ehhez szükséges eszköz egy miniatűr digitális adó-vevőt tartalmazó beültethető mikrochip lenne, az ára-

mot pedig a személy izmainak mozgása biztosítaná elektromechanikusan. Az Applied Digital Solutions (ADS) szerezte meg ennek a technikának a szabadalmi jogait, melyet ők Digital Angel-nek, azaz Digitális Angyalnak neveztek el. Az ADS szerint ez a technika „az emberek széles körű azonosítására, nyomon követésére és megtalálására" használható. A készülék adatokat sugároz és vesz, és folyamatosan nyomon követhető globális helyzetmeghatározó műholdak (GPS) segítségével.

Sokan megbotránkoztak ezen a „Fenevad bélyege" fele vivő lépésen és a cég által választott néven, melyet egyesek Digital Devilként, vagyis Digitális Ördögként emlegetnek. Dr. Carl Sanders professzor 1968-ban lett annak a projektnek a vezetője, amelyik az első kísérletet hajtotta végre a beültethető mikrochip emberi felhasználására. Bár a terven dolgozóknak azt mondták, hogy a mikrochip orvosi célokat szolgál, később rájöttek, hogy kifejlesztésének igazi oka emberi azonosítás volt.

A mikrochip a testhőmérséklet változása által töltődik fel. Ijesztő, hogy migrénes fejfájásokra, viselkedésmódosításra, feldobásra/letörésre, szexuális stimulánsként és elkedvetlenítőként is használható, egyszóval agykontrollra. Sanders most attól tart, hogy a chipet rossz célokra fogják felhasználni. Úgy véli, hogy a mikrochip lesz a „pozitív azonosító és a Fenevad bélyege".

A közvetlen ember-számítógép kapcsolat nem feltevés, hanem valóság. A híradások arról számolnak be, hogy az amerikai hadsereg olyan elektronikus szerkezeteket tesztel, amelyek valakinek a fejére téve vagy ahhoz közel helyezve, érzékelik az illető agyhullámait. Vadászrepülőpilótákon is kipróbálták. Mikor a pilóta arra gondol, hogy kibiztosítja és kilövi a levegő-levegő rakétát, gondolatait

elolvasva a készülék elvégzi a feladatot: kibiztosítja és kilövi a lövedéket. De mi lesz, ha a folyamat megfordíthatóvá válik, és a szerkezet mondja meg a pilótának, hogy mit csináljon?

Olyan chipek kifejlesztésén dolgoznak most az USA-ban, melyek az emberi agyba beültetve hozzákapcsolódhatnak az agy ideghálózatához, lehetővé téve az egyén gondolatainak és cselekedeteinek az irányítását kívülről. Még a kutatók és a kormánytisztviselők is „iszonyatosnak", „Frankenstein-szerű fegyvernek" nevezik ezt a technológiát. Ezeket a találmányokat a Nagy Testvér laboratóriumából valamilyen ördögi célokra használják fel olyan személyek, akik a legfelsőbb hatalomra törekednek. Ebben az elképzelhetetlen gonoszság magja is benne van: emberi agyak tényleges irányítása más emberek által.

Sikeres befolyásolással az embereket hozzászoktatták ahhoz, hogy elfogadják mikrochipek beültetését háziállataikba. A következő lépés az, hogy elfogadtassák velük a beültetéseket bizonyos célcsoportokba, például börtönlakókba, idősekbe, betegekbe, gyerekekbe, és még ki tudja, kikbe. Javaslatok hangzottak el arra is, hogy elektronikusan címkézzék meg a gyerekeket és a tinédzsereket, hogy megleljék őket, ha elvesznek vagy elkóborolnak otthonról. Az is felmerült, hogy a kórházakban a betegekre tett karpereceket mikrochipekkel váltsák fel, hogy az orvosok szkennerrel leolvashassák a páciensek kezéről a kórtörténetüket és az életüket.

Azt is felvetették, hogy miniatűr számítógépeket helyezzenek emberekbe vérnyomásuk, szívverésük, koleszterinszintjük figyelemmel kíséréséhez és szabályozásához, valamint a süketség korrigálásához. Mivel a ránk kényszerített kártyák, mint például a bankkártyák, kártya formátumú

személyi igazolványok, gépjárművezetői engedélyek, útlevelek elveszhetnek vagy ellophatják őket, a mikrochipet a tökéletes megoldásként fogják bemutatni.

Mielőtt a kártyákat felváltaná egy mikrochip, lehetséges, hogy egy egyetemes chipkártyás személyi igazolványt fognak kiosztani mindenkinek. Az ugrás ettől a kártyától a beültethető mikrochipig nem túl nagy. Amerikában már reklámozzák, de már Európában is bemutatták a beültethető chipet. Ez megint egy olyan „a ti érdeketekben tesszük" dolog lesz. Ürügyül azt fogják felhozni, hogy a mikrochip hozzá fog járulni a lopások, a betörések, az illegális bevándorlás és a kábítószer-kereskedelem visszaszorításához, és segítségével elérhetjük majd a bankszámlánkon levő pénzünket bárhonnan a világon. De mások is!

Bár a rendszernek lehetnek előnyei, de túl nagy a lehetőség a vele való visszaélésre, és a személyes szabadság megszűnéséhez vezetne. Nem fogják megmondani, mi minden van beépítve az apró chipbe. Nem fogják elmondani, hogy a mikrochipen keresztül követhetik önöket, megfigyelhetik beszédüket, tetteiket, sőt még az agyukat is kontrollálhatják. Az elektronikus készülékek hordozásával és a számítógéppel való összekapcsolással szemben az emberekben a félelem és irtózás megszüntetése érdekében lázasan dolgoznak a számítógépek miniatürizálásán és a kábel nélküli távközlés kifejlesztésén.

RENDŐRizet

Figyelünk és védünk!

Kiépülőben van egy világméretű megfigyelőrendszer, a Földünk egy óriási koncentrációs táborrá kezd átalakulni. Felderítő műholdak keringenek a Föld körül – szemek az égen –, lent pedig több millió videokamera és más érzékelő van elhelyezve – szemek és fülek a Földön. A számítógépes hálózatok egyre nőnek – ezek alkotják a rendszer agyát. A rögzített jelek ide-oda vándorolnak a rendszerben, információkat küldve az elektronikus szemeknek, hogy jobban lássanak, az elektronikus füleknek, hogy jobban halljanak, és a számítógépes agynak, hogy jobban ellenőrizhesse áldozatait. Nap mint nap figyelemmel kísérhetjük e rendszer megvalósulását, amely maga után vonja az emberek jogainak és szabadságának fokozatos megszüntetését. A számítástechnikát, az orvosi és elektronikai kutatásokat, valamint az ipari technika új vívmányait mind e cél eléréséhez használják fel.

Egy Hitler, Pol Pot, Mao vagy Sztálin szeretett volna a mai Dick Tracy-féle rendőrállam mikrochipjei, térfigyelő kamerái, lézerei, számítógépei, műholdjai, elektromágneses hullámú agykontroll-fegyverei, lehallgatóberendezései és távközlési szerkentyűi birtokában lenni. Dick Tracy természetesen egy jó fiú volt a képregények lapjain, ám rövidesen mindenki szembesülni fog azzal, hogy most a rossz fiúk vannak hatalmon. De akkor már késő lesz!

Rejtett videokamerák és távérzékelők figyelnek minket éjjel és nappal, főleg a nagyobb városokban. Rendőrségek, cégek, üzletek és magánszemélyek videokamerákkal

figyeltetik a következő helyszíneket (városonként eltérő kombinációban), legtöbbször napi 24 órán keresztül: köztereket, közutakat, útkereszteződéseket, autópályákat, iskolákat, egyetemeket, üzleti negyedeket, lakónegyedeket, ipari zónákat, irodaépületeket, kormányépületeket, kórházakat, szállodákat, képtárakat, múzeumokat, bevásárlóközpontokat, üzleteket, postahivatalokat, bankokat, bankautomatákat, vendéglőket, repülőtereket, vonatokat, vasútállomásokat, buszokat, benzinkutakat, határátkelőhelyeket, stadionokat, vagyis az életterünket. Nem véletlen, hogy sorra szüntetik meg az országok közötti határokat, egyszerűen feleslegessé váltak. Hiszen bármerre indul el az ember, mindenhol ugyanazokkal a rendszerelemekkel találkozhat, csak a helyszín, a nyelv, a szokások mások, így valóban nincsen szükség határokra.

A kamerák általában utcai oszlopokra, az épületek tetejére, a bejáratok fölé és a mennyezetre vannak szerelve. Egyes kamerák zoommal rendelkeznek, 360 fokot tudnak körbepásztázni, és nagyon gyenge megvilágításban, akár sötétben is éles képeket készítenek a környezetükről. A kamerák által felvett eseményeket szalagra, digitális lemezekre rögzítik, vagy számítógépes adatbázisokban, nagy teljesítményű szervereken tárolják a későbbi felülvizsgálatig.

Egyes rendszerek számítógépesítettek: felvételeket készítenek bizonyos területeken áthaladó emberekről, és a képeket összehasonlítják az adatbázisban tároltakkal. Ha a kép például egy „körözött" személyé, riasztják a biztonsági szolgálatot. Felfoghatjuk úgy is, hogy minden videokamera egy rendőr szemének felel meg. A kamerák révén ugyanis nagy területen állandó rendőri jelenlét biztosítható.

Egy amerikai szakember szerint ebből a szempontból a folyamatos videokamerás megfigyelés hasonló egy gépi rendőrtiszthez. Képzeljenek el kétezer érintőképernyős noteszgépet, és 8,5 millió eseményt egyetlen adatbázisban! Ennyi számítógép dolgozik a chicagói járőrkocsikban, és ezek segítségével rögzítik a bűncselekményeket a Citizen Law Enforcement Analysis and Reporting (Rendészeti Elemző és Jelentéskészítő) rendszerbe, vagyis a CLEAR-be. Ez a rendszer nem más, mint egy hatalmas relációs adatbázis. Egy hatékony rendőrségnek nem csak azt kell tudnia egy gyanúsítottról, hogy korábban követett-e el valamilyen bűncselekményt, hanem azt is, hogy kiket ismer, és kik ismerik őt.

A legtöbb amerikai nagyvárosi hatóság stratégiai célja az informatika által támogatott rendőrségi munka bevezetése, minél szélesebb körben. A chicagói rendőrség (Chicago Police Department) a New York-i után a második legnagyobb bűnüldöző szervezet Amerikában. A CLEAR adatbázisát 2000 áprilisában indították el, és ma 200 gigabájtnyi adatot tartalmaz. A rendszert 13600 rendőrtiszt és 3000 civil alkalmazott használja.

Rövidesen egész Illinois állam teljes adatrendszerét lecserélik a CLEAR-re. Általában 1200-an használják egyidejűleg, és naponta 7000 keresést hajtanak végre rajta. Ebbe beletartoznak a letartóztatási jelentések, a folyamatban lévő nyomozások állása, a bűnözési statisztikák kerület és utca szerint, a boncolási jegyzőkönyvek, személyek adatlapjai az álnevekkel, becenevekkel és különleges ismertetőjegyekkel, valamint személyzeti adatok, letartóztatások száma rendőrtisztenként és egyéb teljesítménymutatók.

Mivel a CLEAR-t úgy tervezték, hogy integrált, regionális bűnüldözési eszköz legyen, minden rendészeti ügy-

nökségnek, hivatalnak szabad valósidejű hozzáférési lehetőséget adtak. Már több mint 225 ügynökség kapott jogosultságot a használatához. Charles Ramsey, Washington rendőrfőnöke azt nyilatkozta, hogy az Egyesült Államokban a CLEAR a legjobb megoldás.

De hogyan is használják ezt a rendszert? Nyomokat és kapcsolatokat keresnek, nagyjából úgy, mint az utcán, csak sokkal hatékonyabban. Például, ha rákeresnek egy különleges tetoválásra, néhány másodpercen belül számtalan találatot jelez, és minden találathoz nagyítható digitális fénykép tartozik, a tulajdonosának a fotójával együtt. Az „Orosz" becenév keresése egy találatot hoz, de hozzá 14 letartóztatásról szóló jegyzőkönyvet a helyszínek pontos címével, és ez mindjárt le is szűkíti a keresési területet.

Lassú kiépítése ellenére a CLEAR egyre sikeresebb. Több mint 220 önkormányzat kapcsolódott rá eddig a rendszerre, de folyamatosan nő a felhasználók és azok adatainak bázisa. Az FBI, a drogellenes hatóságok és más bűnüldöző szervek is komoly érdeklődést mutatnak iránta. A CLEAR lassan nemzeti modellé válik. A washingtoni rendőrség informatikai vezetője, Phil Graham a következőket nyilatkozta: „Az információ a terrorizmus elleni küzdelem eszköze. A támadások megelőzésére használt adatok ellenőrzése és elemzése akkor hatékony, ha megbízható információkhoz juthatunk. Ebben kulcsfontosságú a CLEAR." De ezek a fejlett szerkentyűk nem ártalmatlan tárgyak tehát, hanem egy rendőrállam lényeges alkotórészei, és a Nagy Testvér mindent látó szemei.

LEHALLGATÁSkálódás

Még a falnak is...!

Elég a „lehallgatás" szót beírni valamelyik internetes keresőbe, s máris magyar, szlovák, orosz és angol nyelvű oldalak tucatjai kínálják (sok esetben illegális) szolgáltatásaikat. Ajánlanak például miniatűr lehallgatókészüléket, amelyet a célszemély lakásában hagyhatunk. Ha nem érjük be hanggal, akár gyufásdoboznyi méretű fényképezőgépet, vagy csillagászati áron ruhagombnál nem nagyobb televíziós kamerát is szerezhetünk. Ha esetleg gondot okozna az illető közelébe férkőzni, műszerek egész sora képes lehallgatni a telefonokat, feltörni az internetes postaládákat. Általában két dolog miatt vásárolják az emberek ezeket a készülékeket: van, aki hűtlen házastársát akarja nyomon követni, mások ipari kémkedést és hírszerzést folytatnak.

Természetesen a barikád túlsó oldalán állók is tökéletesítik a technikát, ideig-óráig előnyhöz juthatnak lehallgatásbiztos telefonok gyártásával. Abszolút biztonságos felszerelés azonban nem létezik. Megesett már, hogy az amerikai Központi Hírszerzésnek (CIA) sikerült lehallgatnia olyan beszélgetéseket, melyeket zárt szobában, csukott ablakok és ajtók mellett folytattak. A vevőberendezést nem a helyiségben, hanem az épülettől néhány száz lépésre helyezték el. Nem kellett hozzá boszorkányság, csak némi jártasság a fizikában.

A hang – így az emberi beszéd is – a levegőben terjed, hangszálaink rezegtetésével tulajdonképpen a levegőt rezegtetjük, s fülünk ezt a rezgést fogja fel. Kevesen gon-

dolnak viszont arra, hogy a rezgést az összes körülöttünk levő tárgy is felfogja, sőt továbbítja is. A szóban forgó CIA-csoportnak tehát nem kellett mást beszereznie, mint egy nagyon jó minőségű mikrofont és egy érzékeny felvevőberendezést, hiszen az ablakok és a kinti levegő is továbbította a bent elhangzott beszélgetést, az emberi fül számára akkor már hallhatatlanul.

Létezik persze kifinomultabb technika is. Nem kell már drága mütyüröket csempészni a célszemély telefonkészülékébe, nem is kell bonyolult rádió adó-vevőkkel vacakolni. Elég egy apró szerkezetet helyezni valamelyik telefonközpontba, hogy az ott átmenő összes beszélgetést rögzíteni tudjuk. Az ilyen típusú lehallgatókészülék elve nagyon egyszerű, egy hetedik osztályos tanuló is elkészítheti a technikaórán. Nem kell hozzá más, mint egy érzékeny tekercs, huzal meg egy jó áramforrás. Minden huzalon – a telefonzsinóron is – áthaladó áram mágneses mezőt gerjeszt, a telefonbeszélgetés hangjának függvényében változó frekvenciával. Már csak a kis tekercset kell a telefonzsinór mellé tenni, és máris rögzíthetjük a beszélgetést.

DIGITÁLentumok

Digitális csodák

Az új, interaktív tévékészülékek nem csak hangok és képek vételére képesek, hanem küldésére is, és rejtett miniatűr kamerákkal vannak felszerelve. De ezek a tulajdonságok nincsenek felsorolva a vevőtájékozató brosúrákon. Ezután a készülékek ugyanúgy nézhetnek minket, mint mi őket. A világ legnagyobb elektronikus háztartási készülékeket gyártó vállalatai és számítástechnikai cégei azt tervezik, hogy teljesen automatizálják háztartásainkat, és nem érdekli őket, hogy akarjuk-e intelligencia és kommunikációs funkciók beépítését a háztartási gépeinkbe vagy sem, a piacon nem lehet majd más fajtát kapni. (Sóvárogva fogunk visszagondolni az akár „áram nélkül is működő", időtálló „Szaratov" hűtőszekrényeinkre, melyeknek csak egyetlen funkciójuk volt: az, hogy lakásunkba hozták a tajga jeges fuvallatát.) Ráadásul annyira beintegrálják ezeket az elektronikus agyakat a gépekbe, hogy ha ki akarná valaki iktatni ezeket a funkciókat (óvatosságból!), akkor a méregdrága készülékek használhatatlanná válnának.

Az egyik fő kérdés az, hova tegyék a ház központi számítógépét. A svéd Electrolux, a világ legnagyobb háztartásigép-gyártója kifejlesztett egy Screenfridge nevű intelligens hűtőszekrényt. A cég azért választotta a hűtőszekrényt a központi számítógép elhelyezésére, mivel otthon az emberek a legtöbb idejüket a konyhában töltik, és a legtöbb út a hűtőhöz vezet. A számítógép a hűtő lábazatában foglal helyet, a lapos, folyadékkristályos, érintésérzékeny képernyő a rajta levő virtuális billentyűzettel az ajtón van.

A hűtőn beépített tévé- és rádióvevő, apró videokamera, mikrofon és hangszóró is van. A ház többi elektronikus berendezéséhez is csatlakoztatható helyi hálózaton keresztül, hogy felügyelje és irányítsa azokat. Az internetre is rá tud lépni, így távolról is irányítható. A hűtőszekrény leltárt készít a benne levő élelmiszerekről az áruk vonalkódjának automatikus leolvasásával, és az elektronikus listát frissíti, valahányszor újabb áru kerül be-, illetve kivételre belőle. Digitális házak prototípusai is elkészültek, az egyik Bill Gates otthona. A benne található összes elektronikus eszköz és háztartási berendezés helyi hálózatba és az internetre van kötve, így helyileg és távolról is irányítható. Oda-vissza!

A reklámok azt hangsúlyozzák, milyen hasznos, hogy a hűtő magától rendel élelmet az interneten keresztül, vagy figyelmeztet, ha elromlott egy háztartási gép; milyen remek, hogy a gyerekeket távolról is figyelemmel követhetjük. Az igazság viszont az, hogy esetleg minket is néznek mások, mikor otthon vagyunk. Vigyázzunk, mert ezeket nem a mi szórakoztatásunkra és kényelmünkre tervezik, hanem profitért, de legfőképpen azért, hogy az év 365 napján, napi 24 órán keresztül követhessék a mozgásunkat, szokásainkat, beszélgetéseinket! Nem mi fogjuk irányítani a házat, hanem mások fognak minket irányítani a házon keresztül.

Ez egy horrorfilmre emlékeztet, amelyben az egyik háznak ördögi lelke volt, és megkísérelte a benne lakókat különféle ravasz módon megölni.

MŰHOLDkórság

Űr-bolyongás

A Föld körül keringő felderítő műholdak folyamatosan küldenek adatokat földi számítógépekhez és fordítva. A hidegháború után az amerikai katonai felderítő műholdakat nem helyezték üzemen kívül, és ma valószínűleg az egész világ megfigyelésére használják. A megfelelő készülékeket hordozó emberek, állatok és tárgyak felderíthetők és nyomon követhetők bármerre a világon globális helymeghatározó műholdak (GPS, GPRS) segítségével.

A terv az, hogy gyakorlatilag mindenkit és minden értékes dolgot ellássanak helyzet-lejelentő mikrochippel. A kereskedelemben részt vevő teherautókat máris műholdak segítségével követik, hogy leellenőrizhessék menetrendjüket, mozgásukat, az autópályák használatát és a feketefuvarokat. Így ki lehet számolni, mennyivel tartoznak az egyes szolgáltatóknak.

A műholdak más földi dolgokat is megfigyelnek, mint például farmon levő állatokat stb. Ha mobiltelefont, miniatűr adó-vevőt tartalmazó chipkártyát vagy más olyan szerkentyűt hordunk magunknál, amely jeleket vesz és küld, ki tudja, hová, akkor mozgásunk a műholdakról követhető. Kártyákkal való fizetés az üzletekben, szállodákban, vendéglőkben; a pénzkiadó automatáknál végzett banki tranzakciók; az autópályák automata fizetőkapuin való áthaladás és bizonyos telefonkártyák használata mind nyomokat hagynak a számítógépes adatbázisokban, amelyek segítségével követni lehet mozgásunkat és cselekedetein-

ket anélkül, hogy elektronikus szemekkel (kamerákkal) néznének minket.

A kormányok folyamatosan egyeztetnek egy új műhold fellövésekor, ha közös célra kívánják hasznosítani, de vannak szigorúan titkos műveletek is, melyek a nyilvánosság kizárása mellett állítanak Föld körüli pályára „keringő szemeket", ezek általában kémműholdak.

Az ilyen bonyolult és drága eszközök elől is el lehet tűnni, a legkezdetlegesebb módszerekkel. Egyszerűen úgy kell élni, mintha az ókorban lennénk. Iktassunk ki minden elektromos és adatátviteli eszközt a környezetünkből, öltözzünk be állatbőrökbe, és költözzünk ki az őserdőbe vagy a sivatagba, egy barlangba! Az élelmünk biztosítva van, a többivel meg ne foglalkozzunk! Így élhet Oszama bin Laden is valószínűleg, mert mivel lehetne magyarázni azt, hogy a mai szupertechnikákkal sem tudták még elfogni... Az biztos, hogy ezek a szuperterroristák jobban tisztában vannak azzal, hogy a hatalom milyen eszközöket használ a megfigyelésre, követésre, az uralkodásukra, mint mi.

A NATO-ban is komoly kutatások folynak a szuperkatonák megalkotásában. Az egyik ilyen a „Digitális katona" projekt. Lényege olyan korszerű technológiai eszközök (intelligens szenzorok, érzékelők, helyzetmeghatározók, adatátviteli eszközök) és alkalmazások komplex rendszerének kifejlesztése, amelyek a „gyalogos katona" számára a XXI. század követelményeinek megfelelő, hatékony támogatást nyújt feladatainak végrehajtásához, és biztosítja a túlélőképesség növelését, funkcionális lehetőségeinek kiterjesztését; a fegyverzet hatásos lőtávolságát minimum 20%-kal meghaladó távolságon biztosítja (bármilyen napszakban és időjárási körülmények között) a célfelderítést.

Legyen képes a látott képet feldolgozható formában továbbítani. Legyen képes a cél rövid (lézeres) megvilágításával annak méteres pontosságú földrajzi koordinátái meghatározására és továbbítására a nagy pontosságú fegyverrendszerek számára.

A speciális érzékelők feladata a katona szervezetének minden (a harc szempontjából lényeges) életműködési adatát figyelni, és azt feldolgozható formában továbbítani (human monitor). Legyen képes a katona ellen alkalmazott célmegjelölő (bemérő) eszközök tevékenységét érzékelni, értékelni, és ellenük aktív ellentevékenységet folytatni; az alkalmazott nukleáris, vegyi anyagok jelenlétét észlelni, és az adatokat értékelni. Legyen képes valósidejű helymeghatározásra, iránymérésre.

A korszerű ruházat legyen golyó-, tűz- és vízálló, hosszabb időn át viselhető, időjáráshoz alkalmazkodó (multiklimatikus), infravörös kisugárzást gátló. A lábbeli legyen képes a gyalogsági aknák hatását annyira lecsökkenteni (repeszállóság), hogy a katona megőrizhesse a harcképességét. A kommunikációs rendszere a sávszélességénél és zavarvédettségénél fogva legyen alkalmas valósidejű kép-, hang- és adatátvitelre. A beépített, korszerű (handfree – érintés nélküli) személyi számítógép képes legyen a kéz használata nélkül is működni a perifériákkal. A célmegjelenítő rendszerrel összhangban legyen képes a megbízható saját-idegen felismerésre. Mint a moziban, a „Tökéletes katona" című filmben. De ez már a valóság.

MUNKAHELYmeghatározás

Dologtalanság

Az alkalmazottak megfigyelése a munkahelyeken napjaink egy fontos kérdése. Brit kutatások szerint a dolgozók interneten töltött idejük egyharmadában a munkához nem kapcsolódó weboldalakat keresnek fel, ami fölös kiadást okoz a vállalatoknak. Vajon mindez feljogosítja a cégeket arra, hogy elektronikus eszközökkel megfigyeljék és ellenőrizzék alkalmazottaikat?

A vállalatok többsége úgy gondolja, jogában áll tudni, mivel töltik idejüket a számítógép előtt ülő alkalmazottak. Vajon pasziánszal múlatják az időt, vagy „humoros" képeket keresnek az interneten, miközben csevegnek ismerőseikkel, és óránként megetetik virtuális tevéjüket? A főnök ideges, mert a vállalat sokat fizet a világháló eléréséért, és úgy gondolja, spórolni tudnának a költségeken, ha a dolgozók a netet kizárólag a munkájukhoz használnák.

A vállalat vezetése ezért beszerez egy kémszoftvert, amelyet föltelepítenek a központi szerverre. A főnök végre mindent tud! Megnézheti, hogy a titkárnője milyen weboldalakat látogat, kiknek ír e-maileket, de akár azt is, vajon a más cégek felé kacsingató dolgozók mely cégeknek küldik el önéletrajzaikat. Mikor kiderül, hogy a főnök beleolvas a levelekbe, felháborodnak az alkalmazottak, többen felmondással fenyegetőznek. A vállalat vezetése azzal védekezik, hogy joga van megfigyelni, mert munkaidőben, és a cég számítógépeit használva interneteztek a dolgozók. De valóban helyes ez az érvelés?

A problémával foglalkozó szakemberek többsége azt mondja, a vállalatoknak igazuk van, nem követnek el törvénytelenséget a megfigyeléssel, hiszen ők állják az internet költségeit, övék a számítógép. Ráadásul, mivel fizetnek alkalmazottaiknak, elvileg ők gazdálkodnak azok munkaidejével is. Ugyanakkor civil szervezetek tiltakoznak, mondván, hogy a vállalat menedzsmentje személyes információk birtokába juthat anélkül, hogy erről a dolgozóknak tudomásuk lenne.

Az egymással folyamatos vitában álló csoportok egyetlen dologban egyetértenek: a munkahelyi megfigyelést szabályozni kell, és erre a világ fejlett országai hajlandóak is. Nagy-Britanniában életbe lépett az a kormányrendelet, amely szigorú feltételek mellett hivatalosan is engedélyezi a vállalatoknak a belső és külső kémkedést.

A cégvezetők feltelepíthetnek különféle elemzőszoftvereket a központi szerverre, adatokat gyűjthetnek arról, hogy munkaidejükben az alkalmazottak milyen weboldalakat kerestek fel, és egy-egy helyen mennyi ideig tartózkodtak. A vállalatok akár e-mail-szűrő szoftvereket is használhatnak, amelyek a meghatározott kulcsszavakat tartalmazó üzeneteket kiemelik a napi elektronikus forgalomból. Azonban a cégeknek csínján kell bánniuk ezekkel az eszközökkel, mert törvénysértést követnek el akkor, ha elolvassák a magánjellegű üzeneteket.

Vannak a világon olyan cégek, amelyek kifejezetten a vállalati megfigyelésre szakosodtak, és ehhez fejlesztenek különféle szoftvereket. Léteznek olyan programok, amelyek bizonyos kifejezésekre, például a vállalati vezetők nevét tartalmazó e-mailekre „ugranak", de lehet kapni olyan szoftvert is, amely egy iroda teljes internetforgalmáról készít jelentéseket.

Nemrég egy skót fejlesztőcég olyan átfogó eszközt készí-

tett, ami megfelelő beállítások mellett a cég dolgozóinak világhálón végzett tevékenységének egészét elemzi, beleértve az e-maileket, az azonnali üzenetküldő rendszereken keresztül továbbított rövid megjegyzéseket, valamint a csevegőszobákban tett hozzászólásokat. Hasonlóan ehhez, egy amerikai cég programcsomagja is átfogó megfigyelési lehetőségeket biztosít, nem csak a hálózaton keresztül továbbított elektronikus adatokat elemzi, de szükség esetén az egyes alkalmazottak számítógépén tárolt dokumentumokat is átfésüli.

Elemzők szerint a vállalati hálózatok fejlődésével és elterjedésével arányosan a kémszoftverek iránt is megnő majd a kereslet. A cégvezetők szeretnének olyan biztonsági rendszereket kiépíteni a munkahelyeiken, amellyel bármikor ellenőrizni tudják, nem küldtek-e ki az alkalmazottak a vállalatra nézve titkos vagy éppen kompromittáló információt valakinek.

Természetesen – miközben a megfigyelőszoftverek egyre bonyolultabbá és „intelligensebbé" válnak –, megjelennek olyan szolgáltatások is, amelyekkel az alkalmazottak kicsúszhatnak a vállalati kémrendszerek hatóköréből. Egy nemrég beindított szolgáltatás a Java-alapú böngészőprogramon keresztül védett, és megfelelően titkosított kapcsolatot használva mutatja meg az egyes weboldalakat a felhasználóknak. A kémszoftverek csupán annyit látnak, hogy a dolgozó számítógépe hosszan kommunikál a safeweb.com internetcímmel, azt azonban képtelenek megállapítani, hogy valójában milyen oldalakat látogatott a titkosított szolgáltatáson keresztül. A cég csak egyet tehet: blokkolja a weboldalt, azonban ezt idővel újra és újra meg kell tennie, hiszen egyre-másra meg fognak jelenni az interneten a hasonló védelmet nyújtó szolgáltatások.

Vannak más perspektívából közelítő megfigyelőszoftverek is, amelyek megmutatják, mi is van az egyes alkalmazottak képernyőjén. Ezeknek a működése egyszerű: a rendszergazdáknak minden munkaállomásra fel kell telepíteniük egy kliensprogramot, ami kérésre elküldi a hálózaton a számítógép monitorán látható képet. A cégek tudtunk nélkül bármikor ránézhetnek, mi történik éppen a számítógépünkön: látják, hogy éppen pasziánszozunk, vagy valami tiltott weboldalt nézegetünk. Egyetlen kattintással „lefényképezhetik" a képernyőtartalmat, ami terhelő bizonyítékként, pár perc elteltével kinyomtatva főnökünk íróasztalára kerül.

Az új szoftverek révén csak otthon, saját számítógépünk előtt ülve érezhetjük biztonságban magunkat, a vállalat előtt semmi sem marad rejtve. Azok, akik hevesen tiltakoznak a megfigyelésnek ennyire nyilvánvaló és részletes formája ellen, azt mondják: az információs társadalom kiteljesedése magával hozta George Orwell rémálmát, a Nagy Testvér megszületését.

A munkahelyi megfigyelés idővel általánossá válik, azonban szigorúan szabályozott keretek közé fog szorulni. Elvileg és törvényileg egyaránt! De gyakorlatilag házon belül bármi megtörténhet. A munkavállalók álláskeresésnél nézni fogják, milyen szintű megfigyelésre számíthatnak leendő munkahelyükön (feltéve, ha erre alkalmat vagy lehetőséget kapnak), és ha tehetik, olyan vállalathoz szegődnek el, ahol munkaadójuk bizalommal viseltetik irántuk.

A jövő behálózott munkahelyein szűrni fogják a weboldalakat, nem lehet majd szexoldalakat nézegetni és tevét etetni, nem lesz mód a kikapcsolódásra. A cégek felismerték ugyanis, hogy hatékony munkát a dolgozóiktól csak

akkor várhatnak el, ha ehhez „megfelelő" légkört és feltételeket teremtenek. Na ez persze nem a tejben és vajban való fürdetést jelenti, hanem a kiszolgáltatottságot, kényszerűséget, a felmondástól, munkanélküliségtől való rettegést, az állandó stresszt, a monoton, robotszerű munkát. Az emberek egyáltalán örülhetnek annak, hogy van munkahelyük.

Az automata jelenlét-nyilvántartás a munkahelyeken kártyák vagy más készülékek segítségével történik. Az alkalmazottak megérkezését, távozását és munkaidejét számítógépes adatbázisokba rögzítik. Ugyanazt a szerkezetet néha épületekbe, irodákba, parkolókba való bejutáshoz, öltözőszekrények, liftek, technikai felszerelések és számítógépes rendszerek használatához is felhasználják, amikor is minden hozzáférés vagy hozzáférési kísérlet nyilvántartásba kerül. A beléptetőrendszerek és a hozzájuk telepített kamerarendszerek együttes használata egyszerűen kizárja az illetéktelen behatolást a védett, illetve megfigyelt területekre.

„Megfigyelőink" nem csak tartózkodási helyünk és mozgásunk nyomon követésében érdekeltek. Beszélgetéseinket és levelezéseinket, szokásainkat, érdeklődési körünket, pénzügyleteinket, sőt még egészségi állapotunkat is figyelemmel szeretnék kísérni. A technika fejlődése megváltoztatta az üzenetváltások lehallgatási módját. A múltban titkos besúgók ezreit alkalmazták a telefonbeszélgetések lehallgatására és lejegyzésére, most ugyanazt a feladatot számítógépes rendszerek látják el, sokkal hatékonyabban.

ÜGYNÖKológia

Kémek és megbízóik

Az elmúlt években az Echelon („harclépcső") nevű globális lehallgatórendszerről kerültek napvilágra részletes adatok. Az Európai Parlament Polgári Szabadságok Bizottsága például jelentést készített erről az elektronikus üzeneteket lehallgatni képes, globális elektronikus kémhálózatról. A jelentés szerint az összes európai telefon, e-mail és fax üzenetváltást lehallgatja az amerikai Nemzetbiztonsági Ügynökség (National Security Agency). A begyűjtött kommunikációs adatokat azután számítógépes programokkal automatikusan kielemzik, „kulcsszavakra" rákeresve.

Az ellenoldal sürgős lépéseket javasol az NSA (az amerikai Nemzetbiztonsági Ügynökség) egyre fokozottabb kémkedése ellen. Ez a világ leghatalmasabb és „leghomályosabb" hírszerző szolgálata, amely Európában, egész Nagy-Britanniára kiterjedő felderítőállomás-hálózatot épített ki az északi féltekén történő kommunikáció lehallgatására.

Kifürkészni az ellenség, az ellenfelek szándékát, helyzetét, erőinek állapotát, az emberiség legősibb „foglalkozásai" közé tartozik. A kínaiak, az egyiptomiak, a görögök, a rómaiak több ezer esztendővel ezelőtt már rendszeresen alkalmazták az ellenség kikémlelésének módszerét. A Bibliában egy konkrét esetet is olvashatunk: „És elküldé őket Mózes a Kánaán földjének megkémlelésére. Nézzétek meg a földet, hogy milyen az; és a népet, mely lakozik azon: erős-é az vagy erőtlen, kevés-é vagy sok?" (Mózes 4. könyve). S ez a kémlelés, a közeli és távoli országok meg-

figyelése, titkaik kifürkészése napjainkra soha nem látott méreteket öltött.

Manapság az eszközök és technikák tökéletesedésével már nem az a módszer, hogy az országok egymáshoz küldik embereiket: „Nézzétek meg a földet!" Most sokkal inkább az a parancs, hogy „hallgassátok meg" rádióforgalmazásaikat, figyeljétek telefonbeszélgetéseiket! A rádió felfedezése óta a szembenálló felek arra törekszenek, hogy egymás adásait lehallgassák, egymás hírrendszereibe betörjenek.

Az első drótnélküli, azaz az üzenet továbbítására rádióhullámokat használó távírót 1896-ban mutatták be, s az akkor áthidalt távolság csupán pár száz méter volt. Néhány év múlva azonban már földrészek között folyt a rádiózás: Marconiék rendszeres szikratávíró-összeköttetést teremtettek Anglia és Kanada között. Most pedig már az űrben keringő műholdakon keresztül folyik az információáramlás real time-ban, vagyis valósidőben, az idő- és távolságkülönbségek ellenére.

A világon 421 kémszervezet működik. Egy bennfentes szerint van olyan ország, amely egymaga százat tart fenn, de hogy melyik, azt ő sem árulta el. Az Egyesült Államokra is jut vagy két tucat, naponta elköltenek több mint 80 millió dollárt. A kémkedés egy igen fontos fegyver. Mint minden fegyvert, ezt is lehet nemes és ártó célokra egyaránt használni. De amíg a közönséges fegyverek önmagukban szűk körben keltenek fel nagyobb érdeklődést, a kémkedést valami különleges romantika, titokzatosság, nemritkán – és nem véletlenül – vérfagyasztó izgalom veszi körül. A hírszerzőkről mindenki tudja, hogy a titkosszolgálatoknál/nak dolgoztak/nak.

Ezek olyan szolgálatok, amelyek beszerzik a híreket,

csak azért, hogy hivatásszerűen eltitkolják azokat. Valami oknál fogva az államok az adófizetők pénzének jelentős részét arra fordítják, hogy eltitkolják előlük a költségesen megszerzett információkat. Az üzleti hírszerzés gyakorlatában ma egyszerre vannak jelen a hagyományos technikák és a legmodernebb eszközök.

Korunk egyik legnagyobb problémája a mobiltelefonok lehallgatása. Ha a mobil lehallgatókészülékkel van ellátva, kikapcsolt állapotban távolról is be lehet kapcsolni, így minden hallható, ami a használója környezetében történik. A készüléket általában nagyobb méretű telefon akkumulátorában helyezik el, a mai, kisebb töltővel rendelkező telefonok erre nem alkalmasak. A készülék jelenlétére utalhat, ha az akkumulátor a szokásosnál jóval hamarabb lemerül, mivel az a készülék a telefon energiaforrását használja. A mobiltelefon jó a helymeghatározáshoz is, ám csak akkor mérhető be, ha be van kapcsolva. Ellenkező esetben csak a bekapcsolt állapot utolsó állomása ismert a hírszerzők számára.

A mobiltelefonok lehallgatása költséges és kockázatos, hiszen gyanú felmerülése esetén az akkumulátor eltávolításával könnyen meg lehet szabadulni a poloskától. Ha alapos a gyanú, hogy preparált telefonunk van, a legegyszerűbb módja a telefon ellenőrzésének, hogy szétszedjük egy másik ugyanolyan telefonnal együtt, amit egy ismerősünktől kértünk kölcsön. Nagyon kicsi a valószínűsége annak, hogy az ismerősünket ugyanúgy lehallgatják, mint esetleg minket. Vizsgáljuk át a szétszedett telefonokat: ha eltérést, valamelyikben plusz „alkatrészt" vagy nem oda illő dolgot látunk meg, az a hunyó. Ilyenkor viccesen szóljunk bele, hogy „Ipiapacs!", és felejtsük el a telefonunkat, úgysincs rá szükségünk!

Ha fontos megbeszélésünk van valakivel, kérjük meg, hogy a telefonját hagyja kint a kocsijában. Vállalati, üzleti megbeszéléseknél azt javaslom, hogy gyűjtsük össze a résztvevők telefonját, és egy általunk megbízott személy egy arra kijelölt helyiségben felügyelje azok működését. Ha valakit hívnak, udvariasan közölje a hívó féllel, hogy a telefon tulajdonosa nem tud épp a telefonhoz jönni.

Ma is használatos a már klasszikusnak számító, tollban elhelyezett lehallgatókészülék kamerával, mikrofonnal felszerelve. 30–50 méteres hatótávolságban tökéletes színes képet és hangot szolgáltat, miközben íróeszközként is jó. Ha gyanúsnak találunk egy ilyen tollat a velünk vagy a társaságunkban lévő személy öltönyzsebében, akkor megkérhetjük, hogy adja már kölcsön a tollát, mert a miénkkel valami történt. Ha megtagadja, és ki sem veszi a zsebéből, joggal feltételezhetjük, hogy valami nem stimmel. Kisméretű, néhány milliméter átmérőjű kamerák, illetve mikrofonok elhelyezhetők a bútorokon, konnektorokba, hosszabbítókba, füstjelzőkbe, órákba, fényképezőgépekbe, de slusszkulcsba vagy táska, ruha egyes részeibe is.

Szintén klasszikusnak számít, és napjainkban is dívik a vezetékes telefonba szerelhető, 1,5 centiméteres, kocka formájú műszer, amely nem a telefonálás során elhangzottakat, hanem a helyiségben zajló beszédet továbbítja, a vezetékes telefonbeszélgetés lehallgatása az előzőekkel ellentétben gyakorlatilag felderíthetetlen. Ez egy központból irányított művelet, amikor is rácsatlakoznak a vezetékre, és magát a beszélgetést hallgatják le. Az ISDN-rendszeren keresztül bonyolított telefonbeszélgetés is lehallgatható, de nagyobb a hírszerzők lebukási esélye, hiszen ebbe a műveletbe a telefonkezelő személyzetet is be kell vonni, illetve be kell szervezni.

Újabb technikának számít például a vízvezetékrendszerbe elhelyezett lehallgatókészülék, amely a fürdőszobában, vécében a gyanútlan beszélő hanghullámait veszi, és továbbítva a jel értelmezhetővé válik.

Ma már általánosnak számít a lézermikrofon, a gamma- vagy infrasugárzás elvén alapuló készülékek használata is. A lézeres lehallgatókészülék előnye, hogy nem szükséges a helyiségben elhelyezni poloskát, mert egy szemben levő helyiségben alkalmazható. A néhány tíz méteres körzetből a tárgyalóterem ablakára irányított készülék érzékeli a helyiségben a beszélgetés során keletkezett, ablaküvegen rezgő hanghullámokat, amit értelmeznek a megbízók.

Az ablaküvegek lehallgatását megakadályozhatjuk speciális szövésű, vastag drapéria függönyökkel belülről, vagy hermetikusan zárható ólomzsalugáterekkel, redőnyökkel kívülről. Gamma-sugár felhasználása révén a fal sem lehet akadály: a tárgyalóterem falának túloldalára elhelyezett készülékek pontosan érzékelik és értelmezik a helyiségben elhangzottakat. A tökéletesen védett helyiségeket nagyon költséges kiépíteni, de megéri.

A fényképezőgépek álcázásában úgyszólván végtelen a – főként német és orosz – tervezők fantáziája: rejtettek már fotómasinát kefébe, öngyújtóba, karórába, nyakkendőtűbe és télikabát gombjába. A rádióadók közül kiemelkedően szellemes a kutyaürüléknek álcázott jeladó – amelyet ha a hidegháborúk idején használtak volna – bombázógépek pilótáit vezette volna célra. Régen a mikrofilmek elrejtésére kiválóan alkalmas volt egy üreges csavar, szög vagy akár pénzérme. Utóbbiból egydolláros és egyrubeles változat is volt a piacon. A napszemüvegbe rejtett videokamerával érdekes illegális felvételeket lehet készíteni.

A titkos ügynökök fegyverei értelemszerűen nem lehet-

nek nagyobbak, mint ami elfér egy titkos zsebben, vagy egy ökölbe szorított kézben. Így nem meglepő, hogy a KGB rúzsba rejtett egylövetűvel szerelte fel kémnőit. „A Halál csókja" becenevű szerkezet 4,5 milliméteres lövedéke közelről végzetes sebet is üthetett. A háromlövetű cigarettatárca még komolyabb fegyvernek tűnik. A miniatűr gyűrűpisztoly a francia titkosszolgálat műhelyét dicséri: XIX. századi kémek hordták, és jól illusztrálja a régi szabályt, miszerint a titkosszolga ne lövöldözzön, hanem próbáljon észrevétlen maradni. Az amerikai OSS például kifejezetten merényletekhez fejlesztette ki a lőpor helyett sűrített gázzal, hangtalanul működő puskáját. Ezek csak ízelítők abból a hosszú listából, mely a kémek, titkos ügynökök által használt „praktikus" eszközöket tartalmazza.

Az alábbi vers egy ismeretlen szerzőtől származik. Nekem nagyon tetszik, mert találó, és tükrözi a jelenlegi helyzetet a világban.

Mondják, félned nem kell,
de most lehullt a lepel,
mert téged valaki figyel.
Itt kém van, hidd el!
Szemek, fülek és test nélküli ebek,
már körülnézni sem merek.
Keresem, kutatom, de nem találom.
Olyan ez, mint egy rossz álom!
Ügynök vagy hírszerző?
Vagy a legkedvesebb barátod Ő?
Hol van az áruló? Ki az a vérszopó, az életmegrontó?
Mi vagy te, csak nem James Bond?
Mennyi az árad, százezer rongy, mondd?!
Hitványságod miatt ezernyi gond.

Miattad testvér is testvérvért ont.
Barát vagy ellenség? Miniszter vagy pap?
A végén egyforma büntetést kap,
mert rájönnek az emberek,
hogy Ők a veszélyes fegyverek.

A köznyelv nem tesz különbséget a kémkedés, a hírszerzés és a felderítés között. Mindhárom fogalom jelölheti azt a titkos tevékenységet, amelynek célja egy másik állam katonai, politikai és gazdasági titkainak megszerzése, akár tisztességes, akár kevésbé tisztességes eszközökkel. A kémek munkája rendkívül nehéz és kockázatokkal teli. Ennek ellenére sokan választják ezt a pályát. Van, aki azt gondolja, hogy azonnal magas jövedelemhez jut. Aláírja a szerződést, és ezzel a saját életét pecsételi meg. Kiszolgáltatottá válik, és ha van családja, akkor vele együtt a családtagjai is, akik valószínűleg semmit nem sejtenek a kettős életéről, ők ugyanolyan potenciális célponttá válnak, mint az illető. De ha szerepet játszik is a pénz, feltehetően csak a különleges képességű ügynökök kapnak magas fizetéseket. Többeket a kalandvágy hajt. Mindig voltak és lesznek olyanok, akiknek életelemük a veszély. Számukra a kémkedés és a vele járó életforma az iskolapadtól a koporsóig tartó kalandot jelenti.

Egy másik kasztot a kémeknek az a fajtája képviseli, akik meggyőződésük ellenére valamilyen zsarolás nyomán kezdenek el dolgozni egy idegen állam titkosszolgálatának. Ilyenek általában a bűnözők közül kerülnek ki, akiket szabadon bocsátásuk ellenében kényszerítenek a kémfeladatok elvégzésére. Ha lebuknak, nem kár értük, és ha feleslegessé váltak, egyszerűen likvidálni lehet őket, mivel amúgy is örökre a börtönben raboskodnának.

Általános gyakorlat a szexuális zsarolás is. A szovjet titkosszolgálat női ügynökei nyugati politikusokat csábították el. Az együttlétről fényképek készültek, és azzal fenyegették meg áldozatukat, hogy vagy kettétörik karrierjüket, vagy számítanak szolgálataikra. Végzetes szenvedély, sértettség, bosszúvágy is közrejátszhat a hírszerző munka vállalásában.

Ezek a motivációk veszélyesek, mert gátlástalanná, érzéketlenné teszik a tulajdonosát. Szinte minden feladatot (ami árthat az „ellenségnek") rájuk lehet bízni. A „nekem úgyis mindegy" felkiáltással vetik bele magukat a munkába, és hazardíroznak. Vagy bejön, vagy nem alapon. Az ilyen ügynökök végzik a faltörő és zárnyitó szerepeket, előkészítve a terepet a kifinomultabb módszerekkel dolgozó ügynököknek. Ezekre a személyekre bízzák az útban álló személyek „félreállítását" is. A módszerek változatosak, melyeket jól előkészítenek, és villámgyorsan hajtanak végre. Észrevétlenül tüntetik el a kiszemelt személyt, vagy öngyilkosságot szimulálnak. Véletlen autóbaleset, ablakból való kizuhanás, különböző gyorsan ható és tökéletesen felszívódó mérgek szerepelnek a repertoárjukban.

A kémkedésnek – éppen Janus-arcú jellegéből fakadóan – kettős megítélése van. A hírszerző munkájáért megbízói részéről komoly elismerésben (anyagiban is) részesül: kitüntetik, hősként emlegetik, neve esetleg a történelem lapjaira is rákerül. Ugyanezt a hírszerzőt (kémet) az ellenfél üldözi, mindenáron igyekszik kézre keríteni, és ha elfogja, a legritkább esetben kap csak kegyelmet.

Az ókor elfogott kémeit rövid úton a másvilágra küldték. Sokan úgy tűntek el, hogy nyomuk sem maradt. Később sem kegyelmeztek a kézre került kémnek, csak azok

maradtak élve, akiktől azt remélték, hogy életükért cserébe gazdát cserélnek, elárulva tényleges megbízóikat. De a háborús körülmények közt foglyul ejtett kémeknek még erre sem volt igazán esélyük. Voltak és vannak köztük titkárok és szobalányok, újságírók és vendégprofesszorok, inasok és üzletemberek. Életük így kettős, a fedőfoglalkozás védelmében gyűjtik információikat.

A kettősség más vonatkozásban is jellemző a kémek egy csoportjára. A kettős kémekről van szó. Ezek – az esetek egy részében – a pénz miatt vállalkoznak az ellenfél vagy egy harmadik állam szolgálatára. Gyakoribb azonban, hogy a letartóztatást csak úgy tudják elkerülni, ha vállalják az ellenfél „kiszolgálását" is. Ez egy borotvaélen táncolás. Nem egy esetben előfordul, hogy a másodállású hírszerző eredeti megbízóit tájékoztatja helyzetéről, s azok készítik elő és juttatják el hozzá az ellenfélnek szánt ál- vagy fél-, esetleg hamis információkat.

Nagyon nehéz eldönteni, hogy kiben bízhatunk, illetve kit bízhatunk meg ilyen feladattal; hogy mikor fordul ellenünk, és szolgáltat információkat az ellenfeleinknek. Ha nem áll módunkban sakkban tartanunk, akkor bármikor megtörténhet az átállása. A lojalizmus (hűség) nem jellemző a mai korunkra, egy szempillantás alatt válhat a bárány vérszomjas farkassá.

A hírszerzés egyik legfontosabb, és egyben legális formája a diplomácia. Mondhatnánk azt is, hogy a diplomata és a kém rokon szakma. Charles Wighton „The Greatest Spies of the World" (A világ legnagyobb kémei) című könyvében azt írja, hogy „A diplomácia és a kémkedés nem más, mint ugyanannak az éremnek a két oldala". A követek (diplomaták) feladata, hogy gyűjtsenek minél több információt a rendelkezésükre álló eszközzel, s ezeket jut-

tassák haza megbízóiknak, akár legális, akár illegális úton. Az a fontos, hogy a küldő fél megtudja, mire készül a másik ország.

A követségek ma is információkat gyűjtenek a fogadó országokról. Ezzel mindkét fél tisztában van, és csak ritkán utasítanak ki diplomatákat kémkedés gyanújával vagy vádjával. A fogadó állam a diplomatát gyakran kitünteti, a kémet viszont, ha elfogja, börtönbe csukja, sőt kivégzi. Ilyen esetekben az érintett ország külügyminisztériuma általában ugyanannyi diplomata azonnali hazatérését kezdeményezi az illető országból, mint ahány diplomatát neki kellett hazahívnia vagy „elvesztenie".

Ma már semmi sem az, aminek látszik. A kémeket minden korban üldözték, s igyekeztek akadályozni a tevékenységüket. Korábban inkább a véletlen segített ártalmatlanná tételükben, de általában valaki elárulta őket. A kémelhárítás a modern államvédelmi szervezetek megalakulásával, a rendőri, illetve a katonai tevékenység speciális területeként alakult ki. Ma már szinte nincsen olyan ország, ahol ne vadásznának kémelhárítók a hírszerző szervezetek ügynökeire. A magányos szuperügynökök (mesterkémek) helyét a hírszerző szervezetek vették át, és ez a hírszerzés nagyüzemi jellegének kialakulásához vezetett.

A hírszerző szervezetek – elsősorban a két nagy világháború, majd a hidegháború körülményei között – olyan hatalmas apparátusokká nőttek, amelyek a legmodernebb technikai berendezéseket, a kémek és elemzők ezreinek szakértelmét és bátorságát használják fel ugyanarra a célra, amint tették ezt az ókorban vagy a középkorban azok a kémek és hírszerzők, akik rátermettségükön és ügyességükön kívül sokszor alig rendelkeztek más eszközzel.

Ebben a szakmában semmi sem félrevezetőbb, mint egy nyilvánvaló tény. Ma az elfogott hírszerzőket a legtöbb állam katonai büntető törvénykönyve háború esetén keményen bünteti. De többnyire csak a mesterkémeket, illetve a hírszerző hálózat vezetőit szokták a legsúlyosabb büntetéssel sújtani. A jobbik esetben kicserélik őket az ellenfél által foglyul ejtett saját hírszerzőikért. Nem háborús időszakban a kémek ellen hozott ítéletek általában enyhébbek. Az úgynevezett „nem hivatalos fedésben" lévő, (vagyis nem a megszokott diplomáciai, katonai, kereskedelmi attaséi megbízással ténykedő) kémek elfogása azonban rendkívül nehéz: ártalmatlan kereskedőként, újságíróként, üzletemberként vagy tudósként élnek a célországban. Beszélik a helyi nyelvet, ténykedésükkel segítik az ország működését, ezért köztiszteletben állnak, széles körű és magas szintű kapcsolatrendszerrel rendelkeznek.

A diplomáciai védettség alatt álló kémek esetében (ha lebuknak) a megoldás egyszerű: kiutasítják őket, és soha többet nem térhetnek vissza. Az Egyesült Államok területén jelenleg az illetékes hatóságok legalább száz olyan orosz kémről tudnak, akik diplomáciai fedésben dolgoznak. A „Time" című amerikai magazin beszámolója szerint a kémelhárításért felelős FBI-szakértők úgy becsülik, hogy a hivatalos „védőernyővel" nem rendelkező spionok létszáma ennek többszöröse is lehet, a KGB utódszervezete olyan aktívnak látszik az USA-ban, mintha csak visszacsöppentünk volna a hidegháború fénykorába.

A kiutasítás azonban kétélű fegyver, mert az ellenkormányok erre válaszul szintén hazaküldik a diplomataként működő ügynököket. Az FBI illetékesei arra gyanakszanak, hogy ismét egy kettős ügynök férkőzött be a soraikba. Minden jel arra utal, hogy megint egy „vakonddal"

van dolguk. Ez pedig több, mint kínos, hiszen alig négy éve leplezték le az orosz zsoldosként dolgozó amerikai beépített kettős ügynököt, a magas beosztású kémelhárító FBI-vezetőt, Robert Hanssent, és akkor abban reménykedtek, hogy megtisztították soraikat. Hanssen letartóztatása után mintegy 50 kémet toloncoltak ki Amerikából, ám azóta megérkezett az utánpótlás...

A veszély megalapozottnak bizonyult az utóbbi évtized egyik legnagyobb kémbotrányában. Illegálisan szerzett üzleti információkat adott tovább az a mérnök, akit a Boeing repülőgépgyártó óriás 1997-ben csábított el hazai versenytársától, a hadiiparban élen járó Lockheed Martintól. Kiderült, hogy a Boeing az illegálisan megszerzett technikai adatokat használta fel ahhoz, hogy beszállítóként részt vehessen az amerikai védelmi minisztérium többmilliárd dolláros rakétaprogramjában. A Pentagon 2003-ban megfosztotta a Boeingot a milliárdos megbízástól, de a nyomozás még ma is tart. Korábban a Boeing annyit ismert el, hogy hétoldalnyi adatot találtak mérnöküknél, de a nyomozás közben a hatóságok még további 25 ezer oldalnyi dokumentumra bukkantak, a gyanúsítottak köre pedig 20 fölé emelkedett.

Újabb és újabb ügynöktörténetekkel leszünk gazdagabbak. Megesik az ilyen. A történelem és a világ már csak így működik. Valamiért jól alszik az, aki aznap valakit elárult olyasvalakinek, akit korábban egyébként már szintén elárult másnak. Ez a rendszer alapja. Sokan kódolva vannak ugyanis a besúgásra, a kémkedésre. A kezdetektől fogva így volt ez. Az információk jönnek, és az információk mennek.

A nemzetbiztonsági hivatal a kormányok irányítása alatt álló, országos hatáskörű, önálló gazdálkodást folytató, a nemzetbiztonsági feladatok végrehajtására létrehozott

fegyveres szerv. Feladatait az Alkotmányban meghatározott alapelvek és követelmények mellett jogszabályok írják elő. Alkotmányos felügyeletét az országgyűlés (parlament vagy a szenátus) látja el. A közvetlen irányítási és felügyeleti jogokat a kormány gyakorolja a Miniszterelnöki Hivatalt vezető miniszteren keresztül.

A mai nemzetbiztonsági szolgálatok sorában a nemzetbiztonsági hivatal sem a mindenkori politikai hatalom eszköze, hanem a polgárok, a nemzet biztonságán őrködő szervezet. Ez a hivatalos megfogalmazás. Tehát az ön és minden állampolgár biztonságán őrködő állami szervezet, melyet önök tartanak fenn, az önök (és mások) megfigyelésére. Pedig önök nem is akarják magukat megfigyeltetni. Ugye?! Akkor hogy is van ez?

ECHELONtológia

Megfigyelés mesterfokon

Napjainkban is nagy jelentőségű az államok hírszerzése számára az ellenség kommunikációjának lehallgatása. Nincs olyan ország a világon, mely – valamilyen formában – ne végezne felderítést, bár ezt mindegyik igyekszik a legnagyobb titokban végezni. Néha azonban fény derül a titokra, s akkor kisebb-nagyobb botrányok közepette a közvélemény is tudomást szerez róla. Ilyen az Echelon-rendszer körül kirobbant botrány is.

A rendszerhez, melyet az amerikai NSA (National Security Agency – Állami Biztonsági Ügynökség) tervezett és felügyel, Új-Zéland, Nagy-Britannia, Kanada és Ausztrália hírszerző szolgálatai is csatlakoztak. Az Echelon (harclépcső) a telefonon, e-mailen, faxon és telexen keresztül folytatott üzenetváltások nagy részét lehallgatja, és percenként kétmillió telefonbeszélgetést bír rögzíteni. A lehallgatott üzeneteket nagyteljesítményű számítógépeken, szervereken tárolja. A speciális programok automatikusan feldolgozzák az írott üzeneteket, előre betáplált kulcsszavak után keresgélve. A kódfejtők és elemzők azután a keresés eredményeit böngészik végig, és kiválogatják a számukra „veszélyt sejtető" üzeneteket. Minden idegen nyelvű üzenetről angol nyelvű fordítás készül. Egyes számítógépprogramok segítségével a telefonbeszélgetésekben – és nem csak az írott üzenetekben – is tudnak kulcsszavak után keresgélni.

Az utóbbi esztendők legnagyobb lehallgatási botrányát egy angol újságíró robbantotta ki, akinek tudomására jutott, hogy Anglia egy eldugott kis településén, Cheshire-ben egy 13 emeletes, titokzatos betonépítmény áll, amely egy gabonatárolóra hasonlít. Az erről készült fotókon jól láthatók a henger alakú építmény tetején elhelyezett különleges (nem szokványos) antennák. A fényképek nyilvánosságra hozatalával az illetékesek kénytelenek voltak elismerni, hogy az objektum falai között titkos lehallgatás és rádiófelderítés (egyszóval kémkedés) folyik.

Valójában mit és kit hallgat le az Anglia közepén lévő állomás? Nos, a kérdésre adandó válasz indította el a lavinát, mivel egyértelmű volt, hogy a „silóból" csak Anglia és a közeli, szomszédos országok rádiói hallgathatók le. De egyáltalán, hogyan épülhetett meg egy ilyen titkos objektum Angliában? Az államvezetésnek tudnia kellett erről. Vagy mégsem?

Az ügy vizsgálatába az Európai Parlament is bekapcsolódott, különleges munkacsoportot hozott létre. A vizsgálat során kiderült, hogy a Cheshire-ihez hasonló állomások működnek szerte a világon, és Angliában még kettő: Nidderdale-ban és Menwith Hillben. Az állomásoknak ugyanaz volt a feladatuk: legkorszerűbb berendezéseik segítségével lehallgatni a rádió- és telefonvonalakat, elolvasni a fax- és e-mail forgalmazásokat.

Ennek a globális lehallgatórendszernek a segítségével folyamatosan és egyidejűleg több ezer összeköttetés megfigyelése lehetséges. A lehallgatórendszer létrehozásáról és üzemeléséről az Egyesült Államok és Anglia a legnagyobb titokban már több évtizeddel ezelőtt szerződést kötött, melyet elneveztek UKUSA COMINT-nek (az Egyesült Királyság és az USA kommunikációs felderítése). Ehhez a szerződéshez két másik, angol nyelvű nemzet is csatlakozott: Kanada és Új-Zéland.

Az Echelont működtető agy, és annak legfontosabb központja a Dictionary (Szótár) fedőnevű adatbázis. Ez az adatbázis kulcsszavak, nevek, szervezetek, a megfigyelés céljából kijelölt ügynökségek, személyek milliónyi adatát tartalmazza, és napról napra terebélyesedik. A lehallgató végpontokon összegyűjtött adatok az Egyesült Államokban lévő NSA-főhadiszállásra, Fort Meade-be kerülnek, ahol a Szótár segítségével szelektálják, értékelik, és a védelem szempontjából fontos adatokat kiemelik. A kiértékelt anyag egy része átkerül az angol katonai felderítő és lehallgató szolgálathoz, a GCHQ-hoz (Government Communications Head Quarters – Állami Távközlési Főhadiszállás).

Ez a mindent lehallgatni tudó „óriási fül" nagy szolgálatot tett már a hidegháború idején is. A 60-as évekig a nemzetközi kommunikációban, a diplomáciai és a katonai hírközlésben a legfontosabb szerepet a rövidhullámú rádiórendszerek alkották. A rövidhullámok az ionoszféráról és a Földről visszaverődve sok-sok ezer kilométer megtételére képesek, de a címzettek és az illetéktelenek egyaránt lehallgathatják, sőt ez meglehetősen egyszerű, nem szükséges hozzá más, mint megfelelő antennák és néhány jó vevőkészülék. Ezt a feladatot gyerekjátéknak tekintette az Echelon.

Az amerikai NSA és az angol GCHQ rendszeresen lehallgatja az európai rövidhullámú telefonvonalakat, egy erre a célra kifejlesztett, különleges antennarendszer, az AN/FLR-9 használatával. Ezeknek a kör alakban elhelyezett antennarendszereknek az átmérője 400 m. Angliai telephelyük Kriknewton, Menwith Hill és Chicksand. Cipruson, Ayios Nikolaos településen felállított berendezéssel figyelik a NATO-országok hírrendszereit, valamint Görögország és Törökország rövidhullámú rádióforgalmát. Az egyik legnagyobb amerikai lehallgatóállomás Virginiában, Vint Hills Farmon működik. Ennek az állomásnak a fő feladata az Egyesült Államokban dolgozó követségek üzenetváltásainak lehallgatása, de innen hallgatják le az Egyesült Királyság rádióforgalmát is.

Az 50-es esztendőkben terjedt el a mikrohullámú rádiózás. Ez forradalmasította a nagy kapacitású, városok közötti kommunikációt. Igen kis teljesítményű adókkal és 1–3 m átmérőjű parabolaantennákkal, melyeket általában magaslatokon helyeztek el, mikroláncot alakítottak ki. Ezeket a mikrohullámú rádióvonalakat műholdak segítségével hallgatták le, kihasználva azon tulajdonságukat, hogy egyenesen terjednek, és egy kis részük kijut a sztratoszférába (világűrbe) is.

A lehallgatást végző CANYON típusú műhold ellenőrző központja a németországi Bad Aiblingben volt. 1978 és 1988 között két CANYON műholdat állítottak Föld körüli pályára, s ezt a vállalkozást az NSA rendkívül eredményesnek könyvelte el. A sikereken felbuzdulva, és a költségeket nem kímélve sorban lőtték fel a kémműholdakat: a CHALET és a VORTEX egymást követték. A média viszont megszimatolta az utóbbi műhold tényleges funkcióját, és ezért gyorsan átkeresztelték a MERCURY névre. Ez a műhold végezte a felderítéseket Irakban, az öbölháború idején. Az ellenőrző központja az angliai Menwith Hillben volt.

A lehallgatástechnikában és az elektronikus felderítésben a legfontosabb feladat a fejlesztés (lépéselőny), a legújabb találmányok és technikai újdonságok azonnali bevetése. A mikro-, valamint a VHF és UHF vonalak lehallgatására a nyolcvanas években két műholdat üzemeltek be. A RHYOLIE és AQUACADE vételét a Földről, távirányítással végezték, az ausztráliai Pine Gap központból.

Az Echelon „óriási fülei" egyre nagyobbak. Kíváncsiságát még ma sem lehet kielégíteni. A frissen fellőtt MAGNUM és az ORION műholdak a telemetriai adatok, a mobil adatközlő vonalak, az URH-rádiók és a mobiltelefonok lehallgatásáért felelősek. Úgy működnek, mint valami óriási, elektronikus porszívók, minden jelet – baráti vagy ellenséges – beszippantanak, és elektronikus agyuk a Szótár keresőszavai alapján szétválogatva, csoportosítva továbbítja a kiértékelt információkat az NSA központ felé.

A földön és az égen minden lehallgatható, de úgy vélhetjük, hogy legalább a tengerek mélyén, a sok száz vagy ezer méteres mélységekben haladó távközlési kábelek biztonságot nyújtanak. Ez naiv képzelgés! Az elektronikus felderítők már régen betörtek ezekbe a tenger alatti telefonvonalakba is. Az 1850-es esztendőkben megkezdődött a földrészeket összekötő, tenger alatti távírókábelek lefektetése, s nem sokkal ezután a telefonkábeleket üzembe helyezték. Míg a kezdetekben ezeken a vezetékeken egyidejűleg csupán néhány száz beszélgetés zajlott, addig a mai, optikai szálas kábeleken másodpercenként öt gigabit digitális információ képes áthaladni, s ez megfelel 60 000 egyidejű csatorna használatának.

A tenger mélyén futó kábelek első konkrét lehallgatása az amerikaiak nevéhez fűződik, 1971 októberében. Egy Halibut nevű tengeralattjáró az Ohotszki-tengeren teljesített szolgálatot, annak a helynek a közelében, ahol a szovjetek katonai telefon- és hírközlési kábele haladt a Kamcsatka félszigetre. A tengeralattjáró rendelkezett egy mélytengeri búvárkamrával. Ennek segítségével felderítették a kábel elhelyezkedését, majd egy merülőberendezéssel megközelítették, s egy (a lehallgatását lehetővé tevő) tekercset helyeztek el rajta. 1972-ben a Halibut visszatért a helyszínre, s ekkor már egy tökéletesebb lehallgatóberendezést szereltek a kábelre, amellyel tíz évig észrevétlenül lehallgatták a szovjet katonai kommunikációt. Ekkor egy volt NSA-alkalmazott felfedte a lehallgatás tényét, és az amerikaiak kénytelenek voltak visszavonulni. A KGB moszkvai múzeumában ma is láthatók ennek az akciónak a tárgyi relikviái.

Egy másik amerikai tengeralattjáró a Barents-tengeren Murmanszk haditengerészeti bázis közelében telepített lehallgatóberendezést egy tenger alatti telefonkábelre. Az USS Parche San Franciscóból indulva, az Északi-sark jégtakarója alatt jutott el a Barents-tengerig. Az akció sikerrel járt, de 1992-ben ezt a lehallgatást is felderítették az oroszok, s így ez is megszűnt működni.

Az Echelon lehallgatási rendszerről ismereteink akkor válnak teljessé, ha a hírközlési műholdak megfigyeléséről is szót ejtünk. A COMSAT műholdakat egy nemzetközi szervezet, a Telecommunications Satellite Organisation (INTELSAT) működteti, nemzetközileg egyeztetett szerződések és forgatókönyv alapján. A fő feladatuk, hogy „point to point" összeköttetéseket és rádióközvetítéseket továbbítsanak. A Földhöz viszonyítva „geostacionárius" pozíciót foglalnak el, azaz a földi bázisról nézve az égen mindig azonos helyen láthatók.

Az első INTELSAT 1967-ben állt szolgálatba, de a fejlődés ezen a területen olyan gyors volt, hogy évente újabb és újabb generációját bocsátották fel. Ez a fajta műhold képes volt 4000 egyidejű telefonbeszélgetés továbbítására, de lehetőség volt ezenkívül telex, távíró, televízió és fakszimile adatok továbbítására is. 1999-ben az INTELSAT már 19 műholdat üzemeltetett.

A távközlési műholdak által továbbított adatok rendszeres figyelése 1971-től kezdődött. Erre a feladatra két

földi vevőállomást építettek és üzemeltek be. Az első két 30 m átmérőjű parabolaantennát az angliai Cornwall-ba, Morwnstow-ba telepítették. Ezek feleltek az atlanti-óceáni és az indiai-óceáni műholdak lehallgatásáért. A másik állomás az Egyesült Államokban, a Washington államban lévő Yakimában működött, ez az állomás a Csendes-óceán térségében lévő műholdak adatforgalmát figyelte. Az államokban egy kisegítő állomást is beüzemeltek, a West Virginia-i Sugar Grove-ban, ennek a mai napig az a feladata, hogy bármilyen pozíciójú műhold lehallgatható legyen.

1985–95 között annyi lehallgatóállomást telepítettek az Egyesült Államokban, Kanadában, Ausztráliában és Új-Zélandon, hogy ezek segítségével 120 különböző műholdat tudtak lehallgatni egyazon időben. Az összes műhold adatforgalmát számokkal nagyon nehéz lenne kifejezni. A világméretű rendszer nagyságát érzékelteti, hogy ezeket zökkenőmentesen kezeli. A fejlesztéseknek pedig még nincsen vége!

A lehallgatott rádióállomások és egyéb távközlési vonalak használói számolnak azzal a lehetőséggel, hogy adásaik lehallgathatók, tehát igyekeznek azokat titkosítani, a szövegeket kódokkal elfedni. A titkosítók és a kódok megfejtői közötti ősi harc mindig is változó eredményű volt: az újabb és nehezebb kódokat csak idő kérdése volt megfejteni, hogy azután ismét új kódok jöjjenek. A jelenlegi ismereteink szerint 1940-től az amerikai NSA az Európában használt valamennyi kriptográfiai rendszert fel bírta törni, s ez a képessége jelentősen hozzájárult a II. világháború kimeneteléhez is.

A háború után egy svájci cég, a Crypto AG került a figyelem középpontjába. Ez a cég rejtjelező és megfejtő berendezések gyártásával a nemzetközi piac vezető cége

lett. Az NSA rövid időn belül szert tett a Crypto AG berendezéseire, melyek segítségével hamarosan 130 ország diplomáciai és katonai hírközlését volt képes megfejteni. A szakemberek véleménye szerint az NSA-nak nem jelent gondot az e-mailek és internet-üzenetek elfogása és megfejtése, valamint azonosítása sem, a Microsoft, a Nestcape és a Lotus szoftverek segítségével.

De nincs legyőzhetetlen lehallgatórendszer. Amit az Echelon könnyedén megtehetett, amikor a távközlési műholdakat hatalmas antennákkal lehallgatta, az ma már sokkal nehezebb és sokkal költségesebb. Az adatok nagy része ma már optikai szálas kábeleken keresztül közlekedik, gyakran a tengerek mélyén. És nehéz olyasmit lehallgatni, ami országok felségterületén halad át.

Ne feledkezzünk meg arról sem, hogy az interneten az adatok ott haladnak, ahol van kapacitás. Ha ön Párizsból Hamburgba küld egy e-mailt, és az európai vonalak bedugultak, a levél Kalifornián át közlekedik. Így az NSA hozzáférhet – ami nem jelenti azt, hogy meg is teszi –, hála azoknak a csatlakozásoknak, amelyek a háló főbb csomópontjain vannak amerikai területen.

Nem szabad megfeledkezni arról, hogy a begyűjtött információkat „szótár-számítógépek” kezelik, amelyek kulcsszavak alapján keresnek és szelektálnak. Ha például ön küld egy e-mailt a rokonának Kanadába, az Echelon csak akkor foglalkozik az üzenetével, ha gyanús a küldemény tartalma. A legjobb védekezés egyébként a titkosítás. Ha a dolog jól működik, a titkosítás észrevehetetlen. Amikor valaki csavarog a neten, a böngészőn keresztül kifigyelhető a tevékenysége. De ha megnézi a bankszámláját, egy olyan kommunikációs csatornába lép be anélkül, hogy észrevenné, amely biztonságos, titkosított.

Ha az egész bolygó e-maileket küldene ugyanazzal a 70 kulcsszóval, egyetlen dologban biztosak lehetünk: az Echelon nem foglalkozna velük. A leghatékonyabb módszer az Echelon működésének visszaszorítására a határozott politikai fellépés. Napjainkban felesleges elmélkednünk olyasvalamin, ami lassanként megszűnik létezni az életünkben, amit régen úgy hívtak, hogy a magánszféra szentsége.

A módszerek nem változtak, csak a tudomány alkotott újabb szuperfegyvereket a magukat mások fölé (szerintük) jogosan vagy (szerintem) jogtalanul helyező csoportok karmaiba. Ennek a történetnek (úgy, mint a könyvemnek) véletlenül megint a fejlett országok bizonyos vezető körei, mi több, kormányai (a Big Brother Gyáróriás mágnásai) a főszereplői. Korunk társadalomtudósai és kultúrantropológusai jogosan állíthatják azt, hogy a hatalom mindig gyanakvó, és ezért lesz ezután is fegyverkezés és haderőreform. Ezért lesznek újabb háborúk, zavargások, leigázások, ahol ki lehet próbálni legálisan (nem laboratóriumi körülmények között) a szupertitkos kreálmányokat.

Egy 1996-ban megjelent könyv a világ békés polgárainak figyelmét az Echelon néven ismert globális megfigyelőrendszer létezésére irányította. Ekkor már az NSA kifejlesztett egy keresőprogramot, NSA Line Eater, azaz „sorevő" néven, ami a neten található anyagokat olvasgatja válogatás nélkül, hogy aztán kiszűrje az Egyesült Államok számára veszélyt jelentő üzeneteket.

„Úriember nem olvassa mások levelét." Henry L. Stimson, az Amerikai Egyesült Államok külügyminisztere ezzel a mondatával zárta be 1929. október 31-én az USA rejtjelező szolgálatának, a Black Chamber-nek a kapuit. Azonban a történelem nem őt igazolta. Stimson állítása (mindannyiunk nagy sajnálatára) a múltban, a jelenben,

és nagy valószínűséggel a jövőben is csak hiú ábránd marad. Nem véletlen az sem, hogy Georg Arthur Orwell angol író „1984" című utópisztikus regényében a következőket írja: „Az embernek annak tudatában kellett élnie, hogy lehallgattak minden hangot, amit kiadott, s a sötétséget leszámítva minden mozdulatát megfigyelték."

Sajnos ma már a bőrünkön érezzük, hogy Stimson felfogása tekinthető utópiának, olyannyira, hogy Orwell fantáziája valóság, és már a sötétség sem akadály. Pontosan a 2000. év egyik világszenzációjaként került nyilvánosságra az a szomorú tény, hogy Földünket évtizedek óta olyan műholdak veszik körül, amelyek lehetővé teszik mindannyiunk lehallgatását.

Ennek a civilek számára hatalmas, átláthatatlan és elképzelhetetlen, ördögi rendszernek a történetéről, felépítéséről szól ez a fejezet. A tényadatok az elmúlt 20–25 évben a nyilvánosság, és főleg a sajtó nyomására napvilágra került dokumentumokból származnak, hiszen maga az Echelon-rendszer ma is a legnagyobb titokban, a titkosszolgálatok felügyelete alatt működik. Már a II. világháború középső szakaszának idején megszületett az Egyesült Királyság és az USA titkosszolgálatai között a BRUSA COMINT (communications intelligence – távközlési hírszerzés) egyezmény, melyet 1943. május 17-én ratifikáltak. Az Egyesült Királyság 1946–47-ben kibővítette a szövetségeseket Kanada, Ausztrália és Új-Zéland háború utáni hírszerző ügynökségeivel. Így jött létre az 1948-ban megkötött titkos UKUSA megállapodás, illetve szövetség, amelynek tartalma és hatálya napjainkban is érvényes.

Az UKUSA szövetség fő koordinátorának (összefogó szervezete) az USA Nemzeti Biztonsági Szolgálatának (NSA) eszközei az USA-ban lefedik a teljes amerikai földrészt. A

szövetség alapító szervezetei: az angol GCHQ (Government Communications Head Quarters – Állami Távközlési Főhadiszállás) Európára, Afrikára és a nyugat-orosz területekre (az Ural-hegységig) figyel, a kanadai CSE (Communications Security Establishment – Távközlés Biztonsági Testület) kezeli az orosz, európai és amerikai északi területek kommunikációját, az ausztrál DSD (Defense Security Directorate – Biztonságvédelmi Igazgatóság) megfigyelési területe Dél-Ázsia és a Csendes-óceán délnyugati, valamint az Indiai-óceán keleti része, és az új-zélandi GCSB (General Communications Security Bureau – Központi Távközlés Biztonsági Iroda) figyeli a déli csendes-óceáni szigeteket. A szerződés jóval későbbi bővítése során kerültek az UKUSA szövetségesek közé Németország, Japán, Norvégia, Dél-Korea és Törökország titkosszolgálatai. A hidegháborús konfliktusok közepette sorra alakultak a katonai és hírszerző ügynökségek, amelyek alapfeladata az információszerzés volt a Kelet-Európa fölé húzott „vasfüggöny túloldaláról".

A legnagyobb ilyen szervezet az NSA volt, amely a Szovjetunió és a kelet-európai szocializmus felbomlása dacára (amely eredetileg fő tevékenységi területe volt!) folyamatosan, sőt exponenciálisan növelte költségvetését, emberi és anyagi erőforrásait. Ez is mutatja, hogy az amerikai Nagy Testvérnek milyen fontos az „elmaradott" keleti blokk napjainkban is. A csecsen hadurak, az afgán drogbárók, az ukrán és az orosz alvilág bűnözői csoportjai, a magyar pornóipar mind-mind potenciális célpontjai a tengerentúli hírszerző szolgálatoknak.

Az NSA foglalkoztatja ma a világon a legtöbb matematikust, a legjobb rejtjelező és rejtjelfejtő szakembereket és csoportokat. Ezek feladata az Államokban és idegen elektronikus kommunikációban megjelenő rejtjelek feltörése, továbbá az így megfejtett üzenetek több mint 100 nyelven történő elemzése. Folyamatosan dolgoznak egy olyan titkosító algoritmus kifejlesztésén, amely biztonságosan védi az USA-kormányszervek kommunikációját. Így érthető az NSA vezető szerepe az UKUSA-szövetségesek között, akik ezt a hatalmas, Föld körüli „információs pajzsot" létrehozták és mai nap is fejlesztik.

Földi megfigyelő bázisok, a tengereken és óceánokon működő kémhajók, tengeralattjárók és szigorúan titkos műholdak tucatjai „figyelik" 30 ezer kilométerrel a fejünk felett az egész Föld, az egész emberiség globális kommunikációs hálózatának forgalmát. A rendszer terve egyszerű és világos: olyan állomások létesítése a Földön és a világűrben, amelyek lehallgatják az összes műholdas, mikrohullámú, mobil és optikai szálas kommunikációs forgalmat, és továbbítják a mérhetetlen mennyiségű információt az Echelon számítógépes központi rendszerébe.

Ez a rendszer a legkorszerűbb hang- és optikai karakterfelismerő (Optical Character Recognation) programokat tartalmazza, valamint olyan kódszavas, illetve kifejezésszótáron alapuló (ennek neve: Echelon Dictionary) szövegfelismerő rendszert, amely kiválogatja a kívánt üzeneteket, és kódolt jelzés kíséretében rögzíti azokat, további elemzés céljára. A lehallgatóállomásokon működő intelligens analizátorok a rögzített beszélgetést vagy dokumentumot összevetik a kulcsszó, illetve kifejezéslistával, és ez alapján továbbítják (vagy sem) a megfelelő hírszerző központba, ahol „illetékesek" eldöntik, hogy szükséges-e a további lehallgatás. Mindez az UKUSA-szövetségesek, elsősorban az NSA fennhatósága alatt működik!

Eredetileg mindössze két földi állomás vette az Intelsat-jeleket: Morwenstow Angliában, és Yakima Washington

államban. Napjainkban az erőforrások jóval kiterjedtebbek. A lehallgatási és megfigyelői kapacitás a finomabb területi és erőforrás-felosztás következtében sokszorosára növekedett.

A Morwenstow állomás közvetlenül szegezi „füleit" (az Intelsat segítségével) az Atlanti- és Indiai-óceánra, Európára, Afrikára és Ázsia nyugati részére. A Yakima állomás célterülete a Csendes-óceán északi féltekére eső része, különös figyelemmel a távol-keleti országokra. A Sugar Grove-i központ (Nyugat-Virginia) lefedi a teljes észak- és dél-amerikai forgalmat. Az ausztráliai DSD állomás Geraldtonban, és az új-zélandi Waihopai GCSB állomás célterülete Ázsia és Csendes-Óceánia déli része. Egy újabb állomás Ascension szigetén (az Atlanti-óceánon, Brazília és Angola között félúton) lefedi a déli félgömb kommunikációját.

A nem INTELSAT műholdakhoz tartozó földi állomások: Menwith Hill (Anglia), Shoal Bay (Ausztrália), Leitrim (Kanada), Bad Aibling (Németország), Misawa (Japán). Az ezekhez tartozó műholdak főleg az orosz és a regionális kommunikációt figyelik. Különös jelentősége van a számtalan rádiófrekvenciás lehallgatóállomásnak, mivel napjaink katonai és civil kommunikációjának jelentős része rádiófrekvencián történik. Az Echelon-hálózat fontosabb rádiófrekvenciás lehallgatóállomásai: Tangimoana (Új-Zéland), Bamaga (Ausztrália) és a közös NSA-GCHQ állomás az Indiai-óceán közepén levő Diego Garcia szigetén.

Menwith Hill az angliai Észak-Yorkshire-ban, Harrogate közelében található. A szakma szerint ez Föld legnagyobb kémbázisa. Közel 25 műholdvevő állomással 1400 amerikai és 350 angol munkatárs dolgozik a bázison. Menwith Hill kiépítése 1951-ig nyúlik vissza, amikor az

USA-légierők és a British War Office bérleti szerződést kötött a földterületre, amely a brit kormány tulajdonát képezte. Az NSA 1966-tól kezdte telepíteni a berendezéseket. Már az 1960-as évek elején az elsők között itt üzemeltették az egyik nagy kapacitású IBM számítógépet.

Az első műholdvevő állomást 1974-ben telepítették Menwith Hillre, alapvetően hírszerzési célokra. Később 8 óriási antennacsoportot építettek, amelyekhez 8 műholdas kommunikációfigyelő rendszer tartozott: STEEPLEBUSH I-II, RUNWAY, PUSHER, MOONPENNY, KNOBSTICKS I-II, GT-6, SILKWORTH. Később további rendszerek kerültek telepítésre (TROUTMAN, ULTRAPURE, TOTALISER, SILVERWEED, RUCKUS).

Ezzel a kiépítettséggel Menwith Hill már egy olyan műholdas megfigyelő-arzenállal rendelkezik, amely képes közvetlenül a saját műholdjaira támaszkodva a földi elektronikus és rádiókommunikáció, adat- és információforgalom minden percét lehallgatni. Az NSA és az UKUSA-szövetségesek tehát sikeresen megvalósították azt az „információs pajzsot" Földünk körül, amelyen pillanatnyilag (az ózonpajzzsal ellentétben) egyetlen pici lyukat sem lehet találni.

A rendszer alapprogramjai sok szempontból már a jövőbe vezetnek. A SILKWORTH szuperszámítógép-rendszer részeként működik például a MAGISTRAND alrendszer, amely vezérli a kulcsszókereső programokat, vagy a PATHFINDER, amely tartalomelemzéssel válogatja szét az üzeneteket és rendezi egy óriási szöveges adatbázisba, amelyből már a dokumentumok (üzenetek) kulcsszavak alapján könnyen hozzáférhetők. Szinte sci-fibe illő alrendszer a VOICECAST, amely hangfelismerő programok segítségével konvertálja a beszélgetéseket szöveges üzenetekké, és

egyéni hangminták alapján a beszélőt azonosítja és tárolja jövőbeni elemzés céljára.

Az Echelon-rendszer napi 24 órában üzemel, a hét minden napján, óránként millió és millió üzenetet feldolgozva. Fontos tudni azonban, hogy az elképzelhetetlen mennyiségű információnak csak kis töredéke kerül tárolásra az elemzések után.

A szótár karbantartásával, aktualizálásával külön munkatársak foglalkoznak, az erre a célra szolgáló programok segítségével (COWBOY, FLINTLOCK stb.), amelyek VAX minikomputerek hálózatán működnek, speciális célú egységekkel kiegészítve. Minden üzenethez (szó, kifejezés, szövegrész), amely a szótárba kerül, egy 4 számjegyű azonosítót rendelnek, amivel beazonosítható az üzenet forrása és tárgya (például: 5535 = japán diplomácia, 8182 = kommunikáció a rejtjelező technikákról). Továbbá minden tárolt adathoz hozzárendelik a dátumot, időt és az állomás kódját, valamint egy kódnevet, amely az ügynökséget azonosítja: ALPHA-ALPHA – AA -(GCHQ), ECHO-ECHO - EE - (DSD), INDIA-INDIA – II - (GCSB), UNIFORM-UNIFORM – UU - (CSE), OSCAR-OSCAR – OO - (NSA). Az így feldolgozott és megjelölt üzenetek továbbításra kerülnek az UKUSA állomások információs idegközpontjába, a PLATFORM számítógépes rendszerbe.

Mindennap összegzik a napi tevékenységet, melyet archiválnak különböző címszavak alatt és formákban:

* *Jelentés,* amely közvetlen, teljes fordítása a lehallgatott üzenetnek;
* *Tömörítvény:* az üzenetben található alapvető információkat emeli ki és sorolja megadott kategóriákba. Ilyen kategória-azonosítók például: MORAY (titkos), SPOKE (titkosabb, mint a MORAY), UMBRA (szigorúan titkos), GAMMA (orosz lehallgatás), DRUID (információtovábbítás nem UKUSA-partnerekhez);
* *Összefoglaló,* az előző két forma keveréke.

Az eddigiekből is kiderült, hogy ma már az UKUSA szövetség éltető, összetartó eleme az Echelon-rendszer. Napjainkban a terrorizmussal szembeni és államellenes tevékenységek elleni védelem miatt újból felértékelődött ez az informatikai szörny, amely egészen új, a civil társadalmat és a politikát érintő felhasználás felé is eltér. Egy STOA (Scientific and Technological Options Assessment – Tudományos és Technológiai Lehetőségek Értékelése) tanulmány rámutatott az Echelon-rendszer használatának sok kényes pontjára, amelyek az USA és az EU kapcsolatát, és főleg állampolgáraikat érzékenyen érintik.

Az Echelon körüli, egyik legnagyobb vihart kavart esemény az 1990-es évek elején került napvilágra, amikor néhány GCHQ-hivatalnok kapcsolatba került a szabadságjogokért küzdő csoportokkal, és 1992-ben nyilatkozatot adtak a London Observernek, miszerint az Echelon-szótárban szerepelnek a következő kifejezések: *Amnesty International, Greenpeace, Christian ministries.* A hírszerző ügynökségek, és így az UKUSA szövetség civil irányban eltorzult tevékenységének igazolására különös „megoldást" találtak, amelynek lényege, hogy a fokozódó terrorizmusra hivatkozva, újradefiniálták a nemzetbiztonság fogalmát, amelybe már beletartoztak a gazdasági, kereskedelmi és részvénytársaságok, és az összes, Földön élő ember is. Tehát az ellenségek köre kibővült önökkel és velem.

Sokszor a gazdasági kémkedés haszonélvezői azok a társaságok (cégek), amelyek segítették az Echelon-rendszer fejlesztését, a hálózat megerősítését. Így tulajdonképpen

„hatalmi védettség" útján kerülhetnek különös, „közvetlen készpénzes" kapcsolatba a hírszerzésen keresztül a hatalom mögött álló politikai pártok és a kormányhoz közel álló üzleti vállalkozások.

Az Echelon-rendszer felhasználásának két fő problémája van: az egyik, hogy a rendszer eredeti, katonai-nemzetbiztonsági rendeltetését kiszélesítették az üzleti, sőt a civil szférára. A másik probléma, hogy ezt a globalizációs mértékkel mérve is elképzelhetetlenül nagy eszköz- és emberi kapacitást néhány kiválasztott (UKUSA-szövetségesek) birtokolja, és hogy erről az óriási információvagyon felhasználásáról végső fokon egyetlen „csúcsszerv" szempontjai döntenek, mégpedig az NSA-é.

Nem csoda tehát, hogy ekkora hatalom birtokában nem sikerül ellenállni a kísértésnek, hogy az információkat politikai és üzleti célokra is felhasználják azok, akiknek azt a rendelkezésére bocsátják. Az alábbi néhány megtörtént eset is a fenti állítást igazolja, ezért mutatok be illusztrációként és gondolatébresztőként párat a számtalan ismert, és talán soha meg nem ismerhető eset közül.

Mike Frost (aki korábban Kanadában kémkedett) beszámol arról, hogy a volt brit miniszterelnök asszony, Margaret Thatcher 1983 februárjában utasítást adott két miniszterének a folyamatos lehallgatására, mivel megingott a megbízhatóságukba vetett bizalma. A megfigyelés az angol (GCHQ) és kanadai (CSE) lehallgatórendszer felhasználásával három hétig történt, majd jelentés készült róla. Maga Mike Frost és szerzőtársa, Michel Graton 1995-ben megjelent cikkükben így írnak erről: „A Thatcher-epizód megmutatja, hogy a GCHQ, akárcsak az NSA, utat talált magának a törvények fölött, és nem tétováznak ezt felhasználni speciális politikai helyzetekben, ha érdekeik úgy kívánják."

Láthatjuk a fenti hírből is, hogy a kormányok vezetői tökéletesen tisztában vannak azzal, hogy mire lehet felhasználni ezt a világméretű rendszert. De ezt velünk nem közlik, csak felhasználják ellenünk. A hálószerűen kiépített rendszer központjait és figyelőállomásait kommunikációs (tv-, rádió-) csatornák bázisainak álcázzák, mert így nem feltűnő a sok speciális antenna az épületek tetején.

Az „információs pajzs" által keltett bizonytalanság nem kíméli a magánembereket sem: egy fiatal gyakorló anyuka telefonon elmesélte a barátnőjének, hogy kisfia homokból bombát készített játszótársaival a játszótéren. A gyanútlan hölgy sosem gondolta volna, hogy a gyermekjáték nem telefontéma. A brit elhárítás számítógépe (összekötve egy telefonvonalakat ellenőrző műholddal) a Szótár alapján felfigyelt a bomba szóra. Beindult az automatikus gépezet, és a beszélgetést rögzítette, majd szöveges formára konvertálta, és megjelenítette az elemzőtiszt monitorján. A tiszt (mivel nem volt biztos abban, hogy a hölgyek nem terrorcselekményt készítenek-e elő, virágnyelven beszélgetve), felvette a hölgyek nevét és telefonszámát a hírszerzés adatbázisába. Az asszonyok neve mellé a következő megjelölés került, örökre: „lehetséges terrorista".

Az Echelon felhasználása „idegen cégek" titkainak kifürkészésére régen ismert volt, ám az 1990-es években ezt „művészi" fokra emelték: 1990-ben az NSA elfogott egy üzenetet, amely a NEC Corp. 200 millió dolláros, műholdgyártásra vonatkozó, küszöbön álló szerződéséről szólt.

Miután ez megfelelő kormányzati csatornák útján az amerikai gyártók tudomására jutott, a NEC és AT&T közötti szerződés meghiúsult.

1993-ban az amerikai elnök megbízta a CIA-t az alacsony károsanyag-kibocsátású autók tervezésével foglalkozó ja-

pán cégek „megfigyelésével". A lehallgatások eredményeként szerzett információkat továbbították a három nagy amerikai autógyárnak, a Fordnak, a General Motorsnak és a Chryslernek.

1994-ben az NSA elfogott egy telefonbeszélgetést, amelyet egy brazil hivatalnok folytatott a francia Thomson céggel egy radarrendszer megvásárlásáról. A feldolgozott információ szintén a „megfelelő csatornákon" keresztül azonnal az amerikai Raytheon céghez került.

Frank Church amerikai szenátor huszonöt évvel ezelőtt megfogalmazott szavai ma is profetikusan hangoznak: „Ugyanakkor, amikor az amerikai emberek lehetőségei gyökeresen megváltozhatnak, és minden amerikai teljes magánéletet élhet, ugyanezek az eszközök teszik lehetővé, hogy minden megfigyelhető legyen (telefonbeszélgetés, távirat, fax, e-mail stb.). Nem lesz egyetlen rejtett hely sem az emberek számára. Ha a kormányzat valaha zsarnoksággá válik, ha egy diktátor kezébe kerül ez az ország, ez a technológiai kapacitás, amelyet a hírszerzés biztosít a kormánynak, tökéletes eszközt ad a kezébe egy totális uralomhoz, amely ellen lehetetlen lesz küzdeni, mert ez a pajzs tökéletes védelmet biztosít a kormánynak. Én nem akarom látni azt az országot, amelyik átmegy ezen a hídon, mert ez a híd olyan szakadékon vezet keresztül, ahonnan nincs visszaút." Ez az idézet akár a könyvem mottója is lehetne.

De az igazi problémát én másban látom. Bárkit, bármikor, bármilyen szinten megfigyelhetnek. Mert képesek rá, az biztos. Azaz bármely magánszemélyről összegyűjthető olyan információ, ami sérti a személyiségi jogait. Kiderülhet, hogy milyen vallás híve, milyen politikai nézeteket vall, milyen a szexuális beállítottsága, melyik civil szervezetnek a tagja, milyen autókat szeret, mi a hobbija, milyen feltétet

kér a pizzájára, mi a kedvenc sportja, időtöltése, mit vásárolt az utóbbi pár évben, milyen reklámokra klikkelt az interneten, vagy bármi egyéb személyes dolog, amire most még nem is gondolunk. És ami ennél is rémisztőbb, hogy valahol a világ másik pontján, egy feneketlen mélységű adatbázisban tárolt csomagocskák mellé előbb-utóbb valakinek eszébe jut a számok és kódok helyett neveket is csatolni.

Ön hogyan érezné magát ezek után? Nagyjából úgy, mint én, vagy Slawomir Mrozek egyperceseinek tipikus főhőse, a kisemberke, aki miután rájön, hogy a feje fölött műholdak röpködnek, és idegen emberek mindent látnak, ami vele vagy körülötte történik, elkezd hirtelen nagyon figyelni az öltözködésére, a mozdulataira, a hajviseletére, és főleg a szavaira. Aztán egy szép napon megunja az egészet, kisétál a városból egy nagy rétre, annak is a közepére. Ott aztán kárörvendő vigyorral letolja a nadrágját, az égnek mereszti a hátsóját, és megmutatja, hogy mit is gondol azokról, akik figyelnek minket. Hát körülbelül így érezhetjük most magunkat mi is. Kár, hogy én nem tudok olyan gúnyosan vigyorogni. Ami most zajlik körülöttünk, nem egy kisregénybe illő történet, nem is egy reality show, ez az eljövendő diktatórikus hatalom életünket beárnyékoló, sötét oldalának előképe.

Az is nyilvánvalóvá vált a számomra, hogy ennek a fejezetnek az írását napjainkban csak abbahagyni lehet, befejezni nem! A tényleges feladata még csak ezután fog kiteljesedni. Az eltelt évtizedeket felfoghatjuk úgy is, mint egy főpróbát. Az eddigi tevékenység is meghökkentő volt számunkra, de ami a közeljövőben várható, azt jelen pillanatban fel sem tudjuk fogni, csak előrevetíteni néhány lehetőséget, mint ahogy Orwell tette, jó rá- és megérző képességgel.

TECHNIKARÁM

Falak nélküli börtön

A fentieken kívül számos más ügynökség és cég is lehallgatja üzenetváltásainkat. A munkáltatók szintén kémkednek a dolgozóik után, lehallgatva telefonbeszélgetéseiket és elolvasva e-mailjeiket. Az Egyesült Államokban „clipper chip"-ek („lehallgatóchip") beszerelését javasolták telefonkészülékekbe, számítógépekbe/modemekbe, faxkészülékekbe és más elektronikus berendezésekbe, hogy a kormány lehallgathassa és megfigyelhesse az üzenetváltásokat.

A tapasztalt terroristák és bűnszervezetek könnyedén kijátszhatnák a „clipper chip"-es lehallgatást, ellenben az lehetővé tenné a diktatórikus kormány államgépezetének, hogy minden telefonbeszélgetést, hitelkártyával való vásárlást, banki tranzakciót, és minden állampolgár távüzenetváltását megfigyelhesse Amerikában, így a kormánynak óriási lehetősége lenne a polgári lakosság manipulációjára és megfélemlítésére.

Érdeklődési körünk sem titok többé, mihelyst az interneten böngészünk, és a számunkra érdekes weblapokat nézegetjük. Remélem, tudják, hogy bármit csinálnak a számítógépen, miközben egy hálózatra vagy az internetre vannak csatlakozva, az lefigyelhető, sőt a számítógépen tárolt adataik sincsenek biztonságban. Vásárlási szokásainkat is kielemzik, mivel bankkártyákkal fizetünk az áruházakban, szállodákban, és mindenhol, ahol lehetőség van rá. Minden pénzügyletünket figyelni akarják, ezért meg fogják szüntetni a készpénzt.

Az egészségi állapotunk is fontos az államhatalomnak. A Yale Egyetem a NASA-val együttműködve egy olyan „értelmes inget" fejlesztett ki katonák számára, amely képes a sebeket észrevenni és kielemezni; a szívverést, oxigénfogyasztást és hasonló életjeleket szemmel követni; az egyén helyzetét meghatározni műholdak segítségével, és azokon keresztül jeleket küldeni. Az ing anyagába üvegszálas vezetékek, érzékelők és egy rádióadó van beleszőve. Ez egy másik példája a látszólag emberbaráti kutatásnak, de képzeljük csak el annak a lehetőségét, hogy a mit sem sejtő áldozatot távolról figyeljék egy ing, farmernadrág stb. által!

Mindannyiunkat ismeretlen és beprogramozott számítógépek figyelnek weblapok nézegetésekor, szörfözés közben. Hollétünk nyilvántartásba kerül, valahányszor bankkártyánkat készpénzkiadó automatákba helyezzük, vagy az autópályák elektronikus fizetőkapuin hajtunk keresztül. A pénzkiadó automaták minden egyes használatakor a bank feljegyzi a tranzakció helyét, dátumát és időpontját.

Tudja-e, hogy a hitelkártyacégek óráról órára nyomon követik minden vásárlását? A cégek azt állítják, hogy ezt két okból teszik: a csalások megelőzésére, és az ügyfelek vásárlási szokásainak a kiderítésére. Térfigyelő videokamerák valószínűleg naponta lefényképeznek bennünket. Ezek ott vannak a bankokban, állami irodaépületekben, gyorsétkezdékben, sőt még a templomokban is. Kereskedelmi műholdak kapcsolódnak rá a számítógépes hálózatra, amelyek elég sasszeműek ahhoz, hogy észrevegyenek valakit – esetleg az élettársával együtt – még a fürdőkádban is. Érdeklődési körünket és vásárlási szokásainkat közzétesszük, valahányszor elektronikus úton rendelünk

meg valamit, miközben egy kereskedelmi weblapot nézegetünk.

Alkalmazottként leolvasók azonosítanak bennünket. Az irodába való belépéshez mágneskártyát használó személy holléte automatikusan feljegyzésre kerül. Rendőrségi rádiószkennerekkel felszerelt hallgatózók lehallgathatják telefonbeszélgetéseinket, és megfejthetik titkos kódjainkat. Minden hitelkártyával fizetett vásárlás egy olyan adatbázisba kerül feljegyzésre, amelybe többek között a rendőrség és az adóhatóság is belenézhet. A munkahelyi e-mailt a munka részének tekintik, amelyet a munkáltatónak joga van elolvasni – és sok főnök ezt meg is teszi. A kormány megpróbálja elhitetni velünk, hogy megfigyelésünk és nyomon követésünk a hasznunkra és védelmünkre szolgál. Azt is értésünkre adják, hogy ha nem tetszik nekünk ez a rendszer, akkor se tehetünk ellene semmit.

A kormány azt is figyeli, hogy merre járunk az autópályákon, és a díjat automatikusan levonja a bankszámlánkról. Ha netán nem akarunk feliratkozni, ki akarnánk játszani a figyelőrendszert, semmi gond: az autópályán elhelyezett, rendszámtábla-felismerő kamerák boldogan lefényképezik a kocsinkat, és pár héten belül a számla megérkezik a postaládánkba.

Ha mostanában valamelyik bevásárlóközpontban, bankban, metróállomáson vagy más „köz"-területen járt, valószínűleg lencsevégre kapták. Ha hívta a brókerét, bankárját, vagy bárki mást, aki nagy cégnél dolgozik, máris archiválták a beszélgetésüket, mert ezeken a helyeken gyakran rögzítenek minden beérkező hívást, „biztonsági okokból". Ha azon gondolkodik, hogy mobiltelefont, vagy akár egy divatos, drótnélküli (hálózati) telefont használjon,

tudnia kell, hogy bármikor bele tudnak hallgatni a telefonbeszélgetésébe.

E-mailt szeretne küldeni? Gondolja meg kétszer is! A számítógépes kalózok bármelyik e-mailt elolvashatják, amelyiket csak akarják. Ugyanakkor ne felejtse el, hogy bírósági döntések alapján munkahelyi e-mailjei a munkáltató tulajdonát képezik, aki bármikor beléjük szimatolhat az ön tudta nélkül, és ezt meg is teszi.

VIRTUÁLIS PÉNZtelenség

Pénz, ami nincs

A világgazdaság lassan pénz nélkülivé válik. Ezt tervezik befolyásos emberek, és óriási összegeket költenek a megvalósítására a befizetett adóinkból. Kiépülőben van az adatbázisok nemzetközileg összekapcsolt globális hálózata, amely rengeteg információt tárol rólunk. A számítástechnika fejlődése tette lehetővé a banküggyletek, adóbefizetések és vásárlások elektronikus úton történő lebonyolítását, és ezek ellenőrzését is. A fizetéseket, állami segélyeket és munkanélküli járadékokat elektronikus úton utalják át a bankszámlákra.

A valódi pénzt így fokozatosan az „elektronikus", azaz „virtuális" pénz váltja fel, ami számítógépeken tárolt számokat jelent. Apránként hozzászoktattak minket, hogy élvezzük az elektronikus rabiga eme kényelmes formáit. Most vagyunk a következő stádiumban: a kártyák és az elektronikus pénz használata kezd kötelezővé válni.

Egyes országokban a pár ezer dollárnál, eurónál nagyobb összegű készpénzügyletek már gyanúsnak minősülnek. Nem véletlenül szorgalmazzák az egységes pénzre való áttérést az uniós országokban. Egységes pénz, egységes ellenőrzés. De így kényszerítik rá a lakosságot a kártyák használatára is.

Bármennyire izgalmasnak (egyszerűnek) tűnik is egyeseknek, ez a számítógépesített gazdaság komoly veszélyt jelent számunkra. Egész életünk számítógépeken köthet ki. A Big Brother Művek tulajdonosai egy egyetemes, számítógépesített, diktatórikus rabszolgarendszer felé vezetnek bennünket.

Az érmék és a papírpénz korszaka rohamosan a vége felé közeledik, és egy pénz nélküli társadalom új korszaka virrad fel. Ha a korszerű elektronikus bankkártyák helyettesíthetik a készpénzt, akkor életünk összes pénzügylete jegyzékbe vehető és tárolható későbbre, és egy pillantás alatt „megfojthatnak" bárkit azok, akiknek hatalmukban áll letiltani az elektronikus pénzhez való hozzáférésünket. A diktatórikus zsarolás és ellenőrzés hihetetlen lehetősége rejlik ebben, de a legtöbb ember mintha nem is venné észre ezeket a jeleket.

A terheléses kártyák veszélye a következő: amíg készpénzt vehetünk fel velük a pénzkiadó automatákból, addig nagyon jól jönnek, hiszen nem kell készpénzt hordanunk magunknál. De a Bankárok világosan kijelentették, hogy a papírpénzt rövid időn belül megszüntetik, és csak elektronikus pénz lesz forgalomban. Ebben az esetben a terheléses kártyák rendszere az emberek teljes ellenőrzésének eszközévé válik.

Például: ha bármilyen okból kifolyólag „nemkívánatos – feketelistás – személynek" vagy az „állam ellenségének" nyilvánít valakit a bank vagy a kormány, akkor elég csupán a számát kitörölni a központi számítógépből, és többé nem lesz képes sem vásárolni, sem eladni, és így arra ítélik, hogy rövid időn belül „eltűnjön". De kérdezem én: hová mehet ez az ember, ha a globális rendszer az egész világot be fogja hálózni?

A pénzügyminisztériumokban, az adóhivatalokban, vagy ki tudja, hol, néhány gombnyomással letilthatják gyakorlatilag mindenét, amije csak van, minden vagyonát, juttatását és járulékait. A készpénz mindig is szabadságot je-

lentett, mert titoktartást és névtelenséget biztosít a tranzakciók során. Ugyanakkor decentralizálást is jelent. Valamely személy pénzügyeinek az ellenőrzése életének az ellenőrzését is jelenti, és az „urak" tisztában vannak ezzel. A lakosság követéséhez, megfigyeléséhez és ellenőrzéséhez jól jön a készpénz kiküszöbölése.

A cél egy pénz nélküli társadalom, ahol minden tranzakciót számítógépes banki rendszeren kényszerítenek keresztül. A bankok támogatják ezeket a terheléses kártyákat. Nekik semmi joguk sincs ahhoz, hogy az egész világ pénzrendszerét kicseréljék egy ellenőrzött kártyarendszerrel. Mégis ezt kívánják megvalósítani a felsőbb akarat nyomásának engedelmeskedve. A bankkártyák teljes, és az egész világra kiterjedő diktatúrához vezetnek. A bankkártyákkal ellentétben a készpénz, vagyis a papírpénz nagy szabadságot biztosít nekünk, mert nem kell kiteregetnünk magánéletünket az azonosításhoz, valamint a termékek és szolgáltatások megvásárlásához.

A kormány ruházta fel a bankokat azzal a hatalommal, hogy pénzt csináljanak, és elosszák azt. A Bankárok azzal dicsekednek, hogy hamarosan kiiktatják a papírpénzt. De azzal nem, hogy ez lehetőséget ad számukra, hogy bármikor átírhassák az összegeket a bankszámláinkon. Bankszámláinkat át fogják tudni alakítani készpénzesről (akár) debit kártyásra. Azt állítják, hogy így meg lehet szüntetni a csalásokat. De pontosan a Bankárok viszik véghez a történelem legnagyobb csalását, és a szemünk láttára. Kiveszik a papírpénzt a zsebünkből, ami jól szolgált eddig bennünket, és olyan kártyákkal helyettesítik, amelyek közlik a számítógéppel fényképünket, számunkat, és más személyes adatainkat.

Eddig csak a híres emberek arcképét lehetett látni a

bankjegyeken, most már a miénk is ott lesz. A világ összes tolvaja és szélhámosa, minden rendőre vadászhat ránk. Mindannyiunkat a kártyáinkhoz akarnak láncolni, és függőségi viszonyban tartani.

Számos pénzügyi szakértő már régóta egy globális tőzsdeösszeomlást jósol. Az lehetőséget teremtene a készpénz kiiktatására, és egy még jobban elrabszolgásító, centralizált gazdasági rend megvalósítására. Ha bekövetkezik ez a világméretű tőzsdecsőd, akkor azt valószínűleg a színfalak mögött, tudatosan tervezték meg (előre). Spontaneitás kizárva! Az embereket először bele fogják kényszeríteni egy új, számítógépesített, nemzetközi azonosítási rendszerbe – infrastruktúrába –, amelyben a digitálissá átalakított személyes adatok számítógépre vitelük után azonnal elolvashatóak lesznek bárhonnan a világon.

A rendszer működése érdekében mindenkinek egy csúcstechnikájú azonosító kártyát fognak kiosztani. Röviddel azután minden létező személyi igazolványt, terheléses bankkártyát, gépjárművezetői engedélyt és hitelkártyát összevonnak egyetlen, technológiailag fejlett, többféle használatra alkalmas chipkártyába, amelyen a chip elektronikus pénzt és személyazonosító információkat fog tárolni. Ezzel majdnem egyidejűleg a világ pénz nélkülivé, és minden pénznem törvénytelenné fog válni, tehát csak számítógépeken keresztül lehet majd venni és eladni, csupán a kibertérben keringő számokkal. Azután azt fogják mondani, hogy az új kártyák könnyen elveszíthetők és ellophatók, és így mi működésképtelenné válhatunk.

Az utolsó lépésben a Nagy Testvér megoldást fog ajánlani ezekre a problémákra. Rá akar venni minket arra, hogy egy azonosítási kártyákat helyettesítő, a kéz bőre alá beültetendő azonosítási biochip-válaszjeladót hordjunk a tes-

tünkben. Anélkül senki sem fog tudni bármit is venni vagy eladni. Az eszközök és a rendszerek már készen állnak ehhez az ördögi tervhez. Tehát itt jön a tökéletes megoldás: az embereket személyesen összekapcsolni a kártyájukkal úgy, hogy ne veszíthessék azt el! És íme: beültetnek egy számítógépes mikrochipet az emberek bőre alá, hogy a létfontosságú statisztikákat bárhol, bármikor, bármilyen távolságból leolvashassák egy elektronikus szkennerrel.

Mivel mindenkiről mindent tudni fognak, minden készen fog állni egy olyan kormány létrehozásához, amely mindenki mozgását ellenőrizni akarja. A bankok jelenleg kampányt folytatnak, hogy az emberek féljenek a tolvajoktól, azonkívül ezernyi tanácsot adnak az embereknek kártyáik megvédésére. De a tolvajoktól való félelmet a bankok csak egy cél érdekében éltetik: el akarják fogadtatni a közvéleménnyel a mikrochipek beültetését emberek kezébe, hogy ezekkel váltsák fel a mikrochipeket tartalmazó terheléses kártyákat. A Föld gazdaságát csak egyféleképpen lehet ennyire ellenőrizni, éspedig ha minden készpénzt kiiktatnak a társadalomból. Mert ha a készpénz megmaradna, senki sem tudna ránk erőszakolni egy ilyen szigorú adás-vételi rendszert.

SZ.I.G.azolvány

Személytelen személyiségek

A Globális Terv másik alkotórésze az, hogy a világon mindenki – lehetőleg a megszületésekor – kapjon egy rányomtatott személyes adatokkal, vonalkóddal, és valószínűleg mágnescsíkkal ellátott, kártya formátumú, fényképes, egyetemes biometrikus személyi igazolványt. A kártyába ágyazott, áttetsző mikrochip tulajdonképpen egy miniatűr számítógép, több gigabyte digitálissá átalakított adatot fog tartalmazni a tulajdonosról: fényképét, ujjlenyomatát, talplenyomatát, íriszének mintázatát, DNS-genotípusát, fehérvérsejt antigén adatait, és más személyes információkat. Ez a miniatűr számítógépkártya a személyazonosság megállapítására, és az adott személyről nemzetközileg összekapcsolt számítógépes hálózatok adatbázisaiban tárolt összes adat elérésére fog szolgálni.

Az állampolgárok személyi igazolványaikat az egész világon létrehozandó, szigorúan védett, számítógépesített kártyakiadó központoktól fogják megkapni, ahol fizikai jellegzetességeiket le fogják mérni, digitálissá alakítják és számítógépre viszik.

Ezt a személyi igazolvány kártyát később esetleg felváltja egy beültethető mikrochip vagy biochip. A kártyát kezelő teljes hardver- és szoftverrendszer alapjai már élnek, és folyamatosan fejlesztik. A világ közigazgatási és egyéb adatbázisai már most is össze vannak kötve hatalmas számítógépes hálózatokon keresztül. Így lehetséges például az (egyáltalán elgondolkozott már azon?), hogy ha bárhová utazik a nagyvilágban, mindenhol fizethet ugyan-

azzal a bankkártyával. A rendszer különböző nyelvű adatokat fog összegyűjteni és kielemezni, melyek minden lehetséges forrásból, például bankoktól, hivataloktól, hírszerző szolgálatoktól, rendőri és katonai egységektől, vállalatoktól, áruházaktól, iskoláktól, a világszerte elhelyezett több millió távolsági biometrikus érzékelőtől, valamint a műholdaktól fognak beérkezni.

Már most is rengeteg számítógépes érzékelő van elhelyezve a világ országaiban, melyek elektronikus üzeneteket küldenek az amerikai Nemzetbiztonsági Ügynökségnek (NSA), és más hírszerző szolgálatoknak. A műholdak olyan kamerákkal vannak felszerelve, amelyek a Földön levő pár centiméteres tárgyakról is tudnak felvételeket készíteni, a képeket pedig folyamatosan elküldik a Földön levő számítógépeknek. Ezek a műholdak üzeneteket váltanak a Földön levő érzékelőkkel, és így bárkinek a mozgását követni tudják, akinél például egy egyetemes biometrikus kártya, vagy egy miniatűr adó-vevőt tartalmazó, beültetett mikrochip van.

A kártya rengeteg állami és civil adatbázissal fog kapcsolatban állni, és a különböző szervek nem csak a kártyán levő személyes adatok leolvasására lesznek képesek, hanem azok megváltoztatására is. A kártya nélkül nem vásárolhat majd senki, nem tud állami támogatást kapni, orvosi ellátásban részesülni, banktranzakciókat elvégezni stb. A kártya többek között „elektronikus", „digitális", azaz „virtuális" pénzként is működni fog az eljövendő, pénz nélküli társadalomban.

Az EMV 'Chip és PIN' infrastruktúrába történt befektetést felhasználva a Visa érintés nélküli módszere lehetővé teszi a fogyasztók számára, hogy ha a kártyát egyszerűen a terminálhoz közelítik, a fizetés fél másodpercnél rövidebb idő alatt megvalósul. A módszert egy standard Visa Smart Debit és érintés nélküli leolvasóhoz társított Ingenico eladási hely segítségével mutatták be, tehát már rendelkezésre áll!

Egy hasonló, a kapcsolat nélküli fizetést lehetővé tevő Near Field Communications (NFC) kagylóhéjjal ellátott Nokia 3220 mobiltelefonnal történő fizetés szintén bemutatásra került. Az új megoldás a kártyatulajdonosoknak a készpénzfizetésnél gyorsabb és biztonságosabb fizetési módszert jelent. Továbbá az érintés nélküli technológia lehetővé teszi a Visa tagbankok számára, hogy a műveletek mennyiségét a nagy mennyiségű, alacsony értékű ügyleteket igénylő vásárlási helyeken történő fokozott mértékű elfogadás és használat megvalósításával növeljék. Ezeken a helyeken, mint például a gyorséttermek, vegyeskereskedések, tömegközlekedés, illetve automaták, hagyományosan a készpénzfizetés dominál. A felhasználóknak komoly előnyt jelent, hogy a pénztáraknál időt takaríthatnak meg. Ezt is köszönjük, mert tudjuk, az idő pénz! Nemsokára már úgyis csak időnk lesz, így ráérünk bármire.

A jelenlegi ISO-14443 Radio Frequency Identification (Rádió Frekvencia Azonosító) (RFID) előírással kombinált EMV technológia lehetővé teszi a kártyatulajdonos számára a kényelem és a biztonság tökéletes egyensúlyát. A kibocsátó bank az érintés nélküli kártya alkalmazásával a legmagasabb érték alatti, valamint a bank által meghatározott és ellenőrzött teljes offline értékhatárig teljesíthető gyors fizetést nyújt. Az azonnali fizetéshez a kártyatulajdonosnak a PIN kódot nem kell megadnia, e helyett a biztonságot egy műveletszámláló biztosítja (a chipen belül), amely abban az esetben, ha a kártyatulajdonos a bank által előzetesen engedélyezett offline limitet eléri, online

módon engedélyezett Chip és PIN műveletet kér, ezzel megakadályozva a kártya elvesztése vagy eltulajdonítása esetén a korlátlan használatot. A nagyobb értékű műveletek teljesítése továbbra is teljes Chip és PIN azonosítással történik.

Várható, hogy a kártyatulajdonosok az érintés nélküli fizetés lehetőségét biztosító kártyát napi rendszerességgel használják majd mind nagyobb, mind pedig kisebb értékű kártyás fizetésekre. Az érintés nélküli fizetés a Near Field Communications (NFC) kagylóhéjjal ellátott Nokia 3220 mobiltelefonnal szintén megvalósítható. Ezt az alkalmazást az NFC kagylóban biztonságosan tárolja egy integrált smart card ellenőrző, amely teljesen kompatibilis a Visa érintés nélküli fizetést biztosító kártyájával. Az NFC lehetővé teszi a mobiltelefonok, valamint egyéb elektronikus berendezések közötti érintés alapú kapcsolatot is.

Pénzügyeink totális kontrollja kihat a gazdaság egészére. Vállalkozásaink ugyanúgy nyitottá válnak megfigyelőink számára. Az egészséges versenyszellem átalakul majd ádáz harccá. Újra a vadnyugat törvénye fog uralkodni: aki előbb süti el a fegyverét, és pontosan céloz, az marad életben.

HACKERingő

A keselyű leszáll

Ha szembejönne az utcán, senkinek nem tűnne fel a negyvenes éveit taposó Kevin David Mitnick. A hétköznapi ember ábrázata mögött viszont egy valódi fenevad lapul. Persze nem egy vérszomjas, hanem egy mindenre elszánt „dögevő", aki bármikor, bárkire lecsaphat! Tőle senki nem lehet biztonságban, misztifikált személye valóság, és csak oda nem megy, ahová ő nem akar. Szerintem irritálja, ha azt híresztelik valamilyen rendszerről, hogy tökéletesen betörésbiztos. A lehetetlen szó hiányzik a szótárából. Született zseni.

Már zsenge tinédzserkorában elkezdte a hekkelést: míg kortársai a lányokat hajtották, ő olyan helyeken kalandozott a számítógépe segítségével, ahová közönséges halandó be sem tehette a lábát. Az első években nem válogatott, mindenhová betört, ahol csak rést talált.

1981 és 1995 között összesen ötször emeltek ellene vádat, többek között a Pacific Bell, a Digital Equipment, egy elektronikus gépjármű-nyilvántartás és az észak-amerikai hadügyi irányító központ, a NORAD rendszereibe való behatolásért. Ez idő alatt többszörös elítéltként szerepelt a bűnügyi nyilvántartásokban. Egy alkalommal próbaidőre bocsátották, de nem bírt magával, ezért 1989-ben egy évre leültették.

Egy 1992-es, próbaidős ítéletet követően szintén megszegte a rá kiszabott ítéletet, ezért három évig kénytelen volt bujkálni az őt üldöző rendőrség és az FBI nyomozói elől. Az elfogásáig számos rendszer látta kárát a bujkálá-

sának, a károsultak között volt a Motorola és a Sun Microsystems is.

Lebukását annak köszönhette, hogy pont egy hackertémában járatos szakértő, Cutomu Simomura gépét törte fel, aki a New York Times oknyomozó újságíró riportere; John Markoff közreműködésével rászabadította Mitnickre az FBI-t. A Condor utoljára 1995-ben került rács mögé, és egészen 1999-ig előzetesben raboskodott. Akkor huszonöt vádpont alapján 68 hónapos elzárásra ítélték.

A ravasz Keselyű vádalkut kötött a szövetségi nyomozókkal, és így a büntetésbe beszámították az előzetesben eltöltött időt is. Mitnick 2000 januárjában szabadult kaliforniai börtönéből. A bíróság 4000 dolláros kártérítés kifizetésére ítélte, amit mellényzsebből kifizetett, viszont az ítélet második fele már keményebben érintette, miszerint három évig nem nyúlhat fegyvereihez: a számítógéphez, a mobiltelefonhoz, de még hordozható telefonkészülékhez sem.

Mitnick a börtönévek során a Julian Rubinstein nagy sikerű könyvéből megismert magyar „viszkis rabló"-éhoz hasonló népszerűségre tett szert. Kiszabadításáért spontán aktivista mozgalmak szerveződtek, a „Free Mitnick" feliratú matricák pedig hosszú ideig hirdették a világ nagyvárosainak utcáin, hogy a Keselyű kalitkában van.

A börtön falai között elhatározta, hogy jó útra tér, és miután kiszabadult, megalapította a Defensive Thinking nevű biztonsági céget, ami ma Mitnick Security Consulting néven áll a megbízók rendelkezésére. Mitnick soha nem hitt a technikában. Az adatvédelmi rendszerek egyre fejlettebbek, és ha az információhoz való hozzáférésről van szó, az igazán hasznos módszer a social engineering, vagyis az emberi tudatlanság, hiszékenység és segítőkészség

kihasználása. Az előző fejezetekben már többször utaltam erre tényre.

Keselyű és barátai nem voltak restek, amikor turkálni kellett a számítástechnikai cégek szemeteszsákjaiban – Mitnick szerint a kis zsákokra érdemes hajtani, mert a nagyobbak a vécéből származnak – és belső használatra szánt telefonkönyvekhez meg jelszavakhoz jutottak hozzá a kukabúvárkodás révén. A szemét egy újrahasznosító számára: aranybánya.

Az emberek hisznek a saját sebezhetetlenségükben. Ezért nem kapcsolják be a biztonsági övet, ezért dohányoznak, és ezért dobják ki a szemétbe a hozzáférési jelszavukat. Ezek mind-mind lyukak azon az emberi tűzfalon. A social engineering 100%-osan hatékony, és a támadónak alig jelent kockázatot, ráadásul független a technikai védelmi eszközök mennyiségétől és minőségétől.

Hogyan védekezhetünk a social engineering ellen? Határozott biztonsági alapelvekkel, az adatok titkosításával, behatolási tesztekkel, folyamatos oktatással, gyakorlati tréningekkel és szituációs gyakorlatokkal.

COMPUTERror

Számítógép-terrorizmus

Annak ellenére, hogy az online elkövetett csalások miatt egyre jobban növekszik a félelem, a legtöbb ilyen visszaélést offline kezdeményezik az elkövetők. Egy elvesztett, ellopott irattárca, benne a csekkfüzettel, vagy a bankkártyákat hordozó pénztárca adja a legtöbb információt a gazemberek számára a csalások elkövetéséhez. Amerikában „csupán" 12%-át teszi ki a felderített bűnügyeknek a számítógépes bűnözés, a privát információkkal való visszaéléshez pedig a legjobb eszköznek a spyware-ek (kémprogramok) bizonyultak.

A legtöbb ember személyes adatait még mindig a hagyományos úton szerzik meg az információtolvajok. A visszaéléseket leggyakrabban barát, rokon, vagy a háztartásban alkalmazott (kertész, házvezető, gyermekfelügyelő) követi el. Az esetek nagy százalékában szinte biztosra vehető, hogy a tettes ismeri az áldozatot.

Aki engedte már számítógép elé a gyerekét, bizonyára beleborzong a következő adatokba. A rendkívül népszerű csevegőfórumokra (úgynevezett chat-szobákba) látogató tíz fiatalból négy bevallja, hogy az interneten megismert – tehát sosem látott (!) – társalkodópartnerek azt kérik, találkozzanak személyesen is. Ezt az ifjak 14%-a meg is teszi, míg a szülőknek csupán 4%-a gondolja úgy, hogy gyermeke elfogadta a randevút.

Bár az interneten leselkedő veszélyekről a legtöbb felnőttnek a pornó jut eszébe, az óvodások-iskolások lelkivilágára az erőszak minden fajtája káros hatással lehet. Ha úgy gondolja, hogy ez túlzás, akkor próbálja ki ön is! Néhány gombnyomás után linkek hosszú sora jelenik meg, és máris választhat, hogy egy iraki túsz lefejezését szeretné videón megnézni, színesben, közelről, vagy állatok megkínzását. A világháló valóban a világot hozza a szobánkba és az életünkbe, annak összes szépségével és gonoszságával együtt.

Az internet – és ezen belül a gyorsabb kapcsolat (ADSL, kábel, széles sáv) – rohamosan terjed a világ minden pontján, a számítógépek „okosabbak" lettek, vannak emberek, akik fölött már uralkodnak is, a fiatalok egyre több időt töltenek a monitorok előtt. A TERV alkotói pontosan ezt akarják elérni.

De szerencsére élnek a Földön olyanok is, akik felkiáltanak, és megpróbálnak szembeszállni az újkori pestis ellen. A Safer Internet Plus (Biztonságosabb Internet Plusz) program is ezt a célt szolgálja. 2005 és 2008 között 45 millió eurót szán a káros és illegális weboldalak elleni küzdelemre.

A nemzetközi összefogásra azért van szükség, mert a világhálón határok nélkül, akadálytalanul áramolnak az információk, így a felelősöket megtalálni és megbüntetni különösen nehéz feladat. Sorra hozzák létre az úgynevezett „forródrótokat", ahol az illegális internettartalmakat lehet bejelenteni (gyermekpornográfia, fajgyűlölet).

Amerikában és néhány EU-tagállamban, ahol már nagyon etikátlanná vált az internet, már most is működik ilyen telefonos szolgálat, ám a cél elterjeszteni és hálózatban összekapcsolni az efféle forródrótokat. Az állampolgároktól kapott információk alapján az internetszolgáltatók és a rendőrség közös erővel próbálja kiszűrni az illegális oldalakat és azok készítőit. Az alapvető cél a felhasználók

„felvértezése" olyan technikai eszközökkel, amelyek korlátozzák a hozzájuk érkező káros tartalmak mennyiségét, vagy éppen lehetővé teszik a már meglévő szűrők tesztelését, speciális kereső- és blokkoló-programokkal.

Egy a lényeg, hogy a számítógépeinken ki lehessen iktatni mindazt, ami gyermekeinkre nézve káros, az erkölcsünket sérti, a jóérzésünkbe belegázol. Biztonságosabb felhasználói környezet kialakításával – a törvények és szabályozások összehangolásával, új etikai kódexek kidolgozásával el lehetne érni, hogy ne csak az utcákon legyen jó a „közbiztonság", hanem az információs világsztrádán is. Ez nem egy „játék határok nélkül", hanem harc, korlátok és határok nélkül.

SZOFTVEResèg

Legyőzöttek

„A nevem Bond, James Bond." A világ leghíresebb kémje így mutatkozik be a filmvásznon. Korunk kémjei, angolul spyware-ek, programok formájában és nem éppen udvariasan, sőt kérdezés és köszönés nélkül lopakodnak be a gyanútlan internetezők gépébe, hogy aztán onnan különböző adatokat lopjanak, miközben a rendszer működését is lelassítják. Azzal, hogy egyre többen egyre több időt töltenek a világhálón, a programok járványként terjednek a világhálón.

A legtöbb felhasználó védettnek hiszi magát a hálóról érkező támadásokkal szemben, holott potenciális célpontok, mivel nem használnak tűzfalat, vírusölő programjaikat ritkán frissítik; közben a számítógépükön spyware-programok tucatjai dolgoznak titokban és láthatatlanul. Ha az előbb felsorolt védelmi eszközökről még nem is hallott, vagy csak felületesen foglalkozott vele, akkor ő már nem is célpont, hanem áldozat. Garantáltan több tíz, de akár száz féreg, vírus és kód is garázdálkodik a gépén. Van, amelyik meg is mutatja magát, de nem ismeri fel, vannak viszont olyanok, amelyek alattomosan megbújva, apránként felemésztik a gép adatbázisait, merevlemezeit, de vannak olyanok is, amelyek egy adott időpontban fognak aktiválódni, és akkor drasztikusan és kegyetlenül tönkreteszik a gépet.

Egy amerikai, kormányzati hátszéllel indított kutatás során az egyik gyanútlan netező gépén több mint ezer kártékony programot találtak a szakemberek. Az America Online

(AOL) internetszolgáltató és az Amerikai Cyberbiztonsági Szövetség (NCSA) által kiadott jelentés szerint a 12 államban megkérdezett 326 felnőtt 77%-a válaszolta azt a telefonos felmérés során, hogy tökéletesen biztonságban érzi magát az interneten fenyegető veszélyekkel szemben.

Ugyanennyien gondolták magukat védve a vírusoktól és a crackerektől egyaránt. Ezzel szemben, amikor a kutatók házhoz mentek ellenőrizni a válaszadók gépeit, leesett az álluk a megdöbbenéstől. A komputerek kétharmadán a vírusirtó programot legalább egy hete nem frissítették, a vizsgált gépek kétharmadának nem volt tűzfala, ebből következően tíz gépből nyolcon találtak valamilyen spywareprogramot (kémszoftverek).

Az amerikai kongresszus a második olyan törvényjavaslatot szavazta meg tavaly, ami törvényen kívül helyezné a felhasználók tevékenységét figyelemmel kísérő, és engedély nélkül információt továbbító szoftvereket. A második indítvány már súlyosabb büntetést helyez kilátásba, amelynek értelmében a kémszoftverek készítői legfeljebb ötéves börtönbüntetéssel sújthatók. A kongresszus ellenszavazat és tartózkodás nélkül fogadta el az „Internet Spyware Prevention Act" néven ismertté vált törvényjavaslatot. Az amerikai Igazságügyi Minisztérium összesen 10 millió dollárt fordít arra, hogy felkutassa a kémszoftvereket készítő egyéneket és csoportokat. A javaslatot támogató szenátorok szerint a kémszoftverek által jelentett veszély egyre nő, éppen ezért súlyos büntetésekkel kell elriasztani a szoftverek készítőit.

Akit tetten érnek a kémszoftver telepítése, a biztonsági beállítások engedély nélkül történő megváltoztatása, vagy akár a felhasználó bizalmas adatainak – az elektronikus postafiók, a telefonszám, netán a bankszámlaszám – eltulajdonítása közben, legfeljebb két év börtönbüntetésre ítélhetik, és öt évet kaphatnak azok, akik behatolnak az áldozat számítógépére, és arról további bűncselekményeket követnek el.

Egy demokrata szenátor kifejtette, hogy határozott fellépés hiányában a kémszoftverek hamarosan a legsúlyosabb fenyegetéssé válhatnak a világhálón. Minden olyan embernek veszélyt jelentenek, akik valamilyen formában kapcsolatban vannak a XX. század nagy vívmányával, a számítógéppel. Egy általa ismertetett felmérés szerint a számítógépek több mint 90%-a tartalmaz valamilyen kémszoftvert. Ez nem akármilyen számadat. Azt mutatja, hogy nem kímélnek senkit ezek a kártékony programok.

Az emberek nem úgy lépnek ki az utcára, hogy bármikor elütheti őket egy autó, így nem is készülnek fel erre a szituációra; így vannak ezzel az internet- és komputerhasználók is. Azonban amikor drasztikusan lelassul az internet-hozzáférés, vagy olyan működési zavarok keletkeznek a gépen, amelyek eddig nem voltak, a megriadt ügyfelek rögtön az internetszolgáltatókhoz, a szoftver- és hardvergyártókhoz fordulnak.

Egy-egy komolyabb spyware-támadási hullám során a felhasználók ezrei szinte leblokkolják a szolgáltatócégek ingyenes vonalait, hogy megtudják a hiba okát. Ez viszont jelentős költségeket okoz a szolgáltatóknak. Egy-két kellemetlen eset után mindenki meggondolja, hogy vegyen-e új terméket attól a gyártótól vagy szolgáltatótól, akivel már pórul járt. Az ilyen cégek azután hiába költenek horribilis összegeket a reklámra: a bizalmatlanság megmarad a vevőkben. És a rossz hírek szélsebesen terjednek. Ennek persze az IT-cégek isszák meg a levét. De ez is a célja az egész háborúnak: egymás működésének az akadályozása, ellehetetlenítése.

Spyware-nek, azaz kémprogramnak azokat a szoftvereket nevezzük, amelyek a felhasználó tudta és engedélye nélkül gyűjtenek személyes adatokat (például e-mail címeket, jelszavakat) a számítógépéről. Leginkább akkor válhat a felhasználó az egyre terjedő kémprogramok áldozatává, ha nem megbízható helyekről tölt le képeket, zenéket, programokat.

A tiltott dolgok mindig kockázattal járnak. A programok zömét olyan oldalakon helyezik el, amelyet a legtöbben látogatnak. A statisztikák szerint az erotikus és pornográf oldalak a legveszélyesebbek, a munkahelyen szörföző férfiak rendszeresen kalandoznak ilyen helyekre. Úgy gondolják, hogy így nem derülhet ki a feleségük által valószínűleg nem támogatott kedvtelésük. Ezzel a gondolkodásmóddal komoly veszélybe sodorják a munkaadójukat, aki azután jogosan korlátozza a hozzáférést a hálóhoz.

A kémprogramok (azonkívül, hogy adatainkat gyűjtik), más kellemetlenségeket is okozhatnak. Szinte biztosra vehetjük, hogy spyware-programmal fertőzött a gépünk, ha a böngészőnk lassabban indul el, akadozik vagy lefagy; ha a kezdőlapunk váratlanul megváltozik anélkül, hogy mi azt akarnánk, és ha a „kedvencek" között új linkek jelennek meg.

Az interneten mindenki számára hozzáférhető programkészítő lépésekkel egy felhasználói szinttel rendelkező amatőr is könnyűszerrel tud olyan mutánsokat létrehozni, amelyek a terjedésükkel riadalmat kelthetnek az IT-piacon. Egyszerű, közismert dolgokra, lépésekre épülnek, majdhogynem szabványosak, sőt automatizálhatók, készíthető ugyanis olyan szoftver is, amely pásztázza a világhálót, keresve a gyenge, betörésre alkalmas pontokat. Az otthoni gépek percek alatt feltörhetők, s ha valaki hazavitte a bizalmas információt, már meg is történt a baj.

A kis- és középvállalatok jellemzően nem védik magukat, a nagyvállalatok rendszergazdái próbálkoznak az optimális óvintézkedések kiépítésével. Kérdés persze, hogy ez milyen mértékben sikerül. Nem mindig a drága védelmi eszközök a legjobbak. A pénzügyi vezetők amúgy is szeretnek ezen spórolni, és általában ezek a költségek az utolsó helyen szerepelnek, hiába ütik az asztalt a szakemberek. A racionálisan gondolkozó pénzügyesek úgy érzik, felesleges költségekről van szó. A prevencióra nagyobb hangsúlyt kellene fektetni, mert egy bénító támadás után már hiába akarják a legdrágább szoftvert megvenni, a baj már megtörtént, lehet, hogy az egész rendszert ki kell hajítani a szemétbe.

A nemzetbiztonsági hivatalokban is úgy vélekednek, hogy az információs háború rendszerint csak akkor tudatosul az emberekben, a vállalkozások vezetőiben, amikor az érzékeny területekre már „betörtek". Hallják a hírekből, hogy nagy és tőkeerős vállalatok rendszereibe, vagy kormányhivatalok központjaiba törnek be a vadászok, és mégsem féltik a saját gépeiket. Márpedig ha a CIA rendszerébe is bementek, akkor a mi rendszerünk gyerekjáték nekik.

Az is aggasztó, hogy az ipari kémkedés egyre inkább az információs bűnözés felé tolódik el. Az informatikai bűnözésen belül egyre nagyobb az ipari kémkedések aránya. Ezen nem csodálkozhatunk, mert amióta a cégek számítógépeken tárolják az információikat, azóta a fő célpontokká az adathordozó eszközök váltak. De higgyék el, még ott is nehéz lépést tartani a hackerekkel, ahol komolyan igyekeznek magukat védeni.

Az operációs rendszerek (pontosan a védelmi erőfeszítések miatt) egyre bonyolultabbak, nincsen idő a hosszabb

tesztekre sem, ezért olyan hibák maradnak bennük, amelyeket a hackerek megtalálnak és fel is használnak. Ők igyekeznek a betöréseiket teljesen hétköznapi, megszokott műveleteknek álcázni, mert így egy átlag felhasználónak nem tűnik fel a jelenlétük. Az ügyes hackert azért sem könnyű tetten érni, mert soha nem a saját számítógépét használja fel a támadásra. Betör például egy egyetemi gépparkba, ahol értelemszerűen nem olyan nagy a védelem, nem figyelik a mozgásokat, s azon keresztül kémkedik. De bármikor el is tüntetheti a naplóbejegyzéseket, így a tevékenysége örökre rejtve marad.

Látva a százszázalékos védelem nehézségét, a védelmi szakemberek már olyan eszközöket is kifejlesztettek, amelyek magukra vonzzák a hackerek figyelmét. Úgy működik, mint a légyfogó. A hálón keringő rossz fiú észleli a felkínált prédát, lecsap rá, és akár hetekig is odaragadhat a sok próbálkozástól. Ezzel elterelhetik a figyelmét a valódi prédáról. Ezt az eljárást a szakma „honey pot"-nak, vagyis mézescsupornak hívja.

A számítógépek támadhatósága gyakran az emberi butaságra és a naivitásra vezethető vissza. Ha egy vállalati dolgozót felhív valaki a munkahelyén, és bemutatkozik, hogy ő a rendszergazda, majd kéri, hogy adja meg a jelszavát, mert kicserélik a PC-jét, és a gépen található adatokat el kell menteni a központi szerveren, akkor szerintem mindenki gondolkodás nélkül asszisztálna ehhez a feladathoz, kiadva a személyes belépési kódokat, biztonsági kulcsokat és jelszavakat. Hiszen mindenki tudja egy jól működő vállalatnál, hogy a gépekhez csak a rendszergazdáknak van joguk hozzányúlni. Ön mit tenne hasonló helyzetben?

Nem győzöm hangsúlyozni, hogy tudatosítani kell az

emberekben: a veszély igenis létezik, ezért a gondolkodásmódunkat át kell formálni, a cégeknél hatékony rendszabályokat kell alkalmazni, be kell tartani és tartatni azokat. Ez nem csak az informatikára igaz, hiszen léteznek az ipari kémkedésnek más formái is.

Amikor valamely országban egy hivatalosan bejegyzett, gazdasági információk gyűjtésével foglalkozó céget egy külföldi vállalat nevében, a konkrét befektetést megelőző időszakban megbíznak a kiszemelt célpont átvilágításával, különféle eszközöket és taktikákat alkalmaznak. Általános gyakorlat, hogy az alkalmazottaknak vagy a volt alkalmazottaknak pénzt kínálnak olyan, gazdaságilag értékes információkért, mint például ár- és ügyféllisták.

De fontosak lehetnek az azonos versenytárgyaláson (tenderen) indulók ajánlatainak részletei is, vagy olyan technológiai újdonságok, melyekkel piacvezető szerepbe kerülhetnek. A milliárdokat érő, új gyógyszerformulák is kedvelt célpontjai az ügynököknek. De ugyanígy megvehetnek stratégiákat vagy cégfelvásárlási terveket is.

Egy viszont biztos: komputertechnológia segítségével és hackerkedéssel jóval kevésbé kockázatos információt lopni, mint valakinek a lefizetésével.

CARNIVOREvans

Az FBI visszavág

Az FBI szakemberei sem tétlenkednek. Ha valahol a világon feltűnik egy új vírus, kód, féreg vagy titkosító eljárás, akkor haladéktalanul nekilátnak annak elemzéséhez és a feltöréséhez. Így került kifejlesztésre egyfajta ellencsapásként a sokat támadott Carnivore-program is, ami az IP (Internet Protocol) adatforgalom hasznos adatait elemzi, a rejtett üzenetekből viszont semmit nem észlel.

A kibertérben üzengető terroristák, kiberbűnözők azzal külön eltüntetnek minden nyomot, hogy az adatcsomagok feladójaként, illetve postásaiként kormányzati hivatalok internetes szerveit jelölik meg, és közel 70 ezer internetes csatornát használhatnak jelenleg. Kiaknázzák az összes, technika adta lehetőséget, valamennyi rendelkezésre álló kommunikációs kaput, na és persze a titkosító és rejtjelező alkalmazásokat is.

Az FBI célja, hogy egy általuk kifejlesztett trójai program segítségével a billentyűzetet figyelő keylogger szoftvert csempésszenek a célszemélyek által használt komputerekbe. A felhasználó leütéseit a program a háttérben figyeli, feljegyzi, és bizonyos időközönként elküldi a hivatalnak. Ezáltal a gépen elmentett, vagy a kommunikációban használt, titkosított fájlok tartalmához az időigényes feltörés helyett közvetlenül a felhasználó saját jelszavával férhetnek hozzá.

Ez a rendszer és program mint számítógépes program nem tesz különbséget ember és ember, felhasználó és felhasználó között. Ott végzi alantas és sunyi munkáját,

ahová küldik a kitalálói. Ha éppen az ön gépére, akkor ne csodálkozzon, mert azt valaki tudatosan, előre megfontolt szándékból telepíti oda. Hogy miért? Hát ez a nagy kérdés!

Ha a történéseket elemezzük, rájöhetünk, hogy rövidesen eljön az idő, amikor már minden gép eleve fertőzötten kerül a felhasználókhoz, gyárilag beleintegrálják az operációs rendszerekbe az információt rögzítő, elemző és küldő programokat. Már most is nagyon nehéz kiigazodni a gépeken futó programokon. Egyelőre csak azok ismerik a hatásmechanizmusukat, és a feltételezhető pusztításukat, akik megalkotják.

Ezeknek a speciális programoknak a megszületéséig az FBI erre a feladatra szakosodott ügynökeinek közvetlenül találkozniuk kellett a célszámítógéppel, vagyis egy keylogger telepítéséhez be kellett hatolniuk a gyanúsított lakásába vagy irodájába. Az FBI által kifejlesztett megfigyelőrendszer közismert neve, illetve fedőneve Cyber Knight, vagyis Kiberlovag.

A programon belül működő gigantikus adatbázis feladata, hogy a szűrőhálón fennakadt e-maileket, a megfigyelt chat-szobák loggjait (bejelentkezéseit), az üzenetküldő programok szóváltásait rögzítse, rendszerezze és tárolja. Az e-mailek begyűjtéséért például a fent említett Carnivore felel. A rendszernek ugyancsak része a titkosítást elemző és feltörő Magic Lantern, vagyis a Csodalámpás nevű program, amely egy keylogger és egy trójai vírus kombinációja.

A keyloggolás, vagyis a klaviatúrán (billentyűzeten) folytatott ügyködés (a leütések) rögzítése egy egyszerű és „oldschool" tolvajmódszer: a felhasználó teljes elektronikus kultúrája, szokásai nyomon követhetők segítségével, a tár-

salgástól a szörfözésen keresztül a jelszavakig. Az állítólagos szakembereket főleg az utóbbiak érdeklik.

A Magic Lantern nem igényel semmiféle fizikális kapcsolatot (vezetékezést), mivel szoftverként jegyzeteli a gépelést, ez a szakma gyors- és gépírója, aki fáradhatatlanul dolgozik éjjel és nappal. A megfigyelni kívánt célponthoz trójai vírus formájában jut el e-mailben vagy egyéb módon.

A loggolást a titkosító programok elindítása aktiválja; ha valaki valamit le akar titkosítani, az valamiért fontos neki, így a loggolónak is, nem beszélve a figyelőkről... A trójai működése közelebbről nem ismert. Nem véletlenül! Elképzelhető, hogy az interneten keresztül azonnal továbbítja a gépelést az FBI-nak, vagy csak megkereséskor küldi az információt, esetleg mindkettő. De ez végül is teljesen mindegy. Csak AZ nem mindegy, hogy az én adataimat küldi el valahová, valakinek.

A rendszeressé vált terrortámadások a kriptográfia és a titkosító szoftverek körül zajló vitában is fordulatot hozhatnak. A privát szféra védelmezői mindeddig sikerrel védték ki, hogy a kormányzat megtiltsa vagy visszafejthetővé tegye a titkosított kommunikációt. Az FBI viszont már régen hangoztatja, hogy a feltörhetetlen titkosítás lehetővé teszi a Hamasz, a Hezbollah és az al-Kaida terrorszervezetek zavartalan kommunikációját.

Ebben van némi igazság, még egyet is érthetnénk vele, ha a nem terrorizmussal és bűnözéssel összefüggő magántitkosításokat békén hagynák. De mivel nem tudják elkülöníteni hitelt érdemlően ezt a két közeget, ezért szerintük inkább minden legyen feltörhető, elolvasható, beazonosítható.

Az általános szolgáltatói rendszerekben használt keresőszoftver-verziók egy óra leforgása alatt körülbelül 6 gigabyte adatot tudtak átfésülni. A Carnivore másodpercenként több millió üzenet szövegében keres. Azért van különbség!

Az FBI számára mindenki gyanúsított, ezzel indokolja a szoftver létjogosultságát. Másképpen képtelen lenne a sok millió e-mail közül kiválogatni a neki oly „kedves" gyanúsítottakét. Az Amerikai Civil Forradalmi Szövetség (ACLU) polgárjogi szervezet azzal érvel, hogy a hivatal mindenkit megfigyel, természetesen csak „a biztonság kedvéért", hogy aztán szabadon használhassa az elfogott és rögzített adatokat, amire akarja.

A függetlenségüket védő civiljogi aktivisták szerint ez a módszer ahhoz hasonlítható, mintha minden telefont válogatás nélkül lehallgatnának, csak azért, hogy megállapítsák, melyik beszélgetésre van szükségük. Irdatlan adatmennyiséget lehet így összegyűjteni, s ezek rendszerezve félelmetes fegyverré válhatnak annak az FBI-nak a kezében, amely nem érti meg a civilek aggodalmát.

Arra hivatkoznak a nyomozó hivatal vezetői, hogy ennek az össznépi e-mail-figyelésnek megvan a jogi alapja, hiszen végső soron csak a telefonos lehallgatás XXI. századi megfelelőjéről van szó. Ezek szerint már az előző században is becsülettel lehallgattak minket, és akkor sem kérdezték meg a véleményünket.

Az illetéktelen adatfelhasználás ellen véd a törvény, a fű alatt gyűjtött bizonyítékokat (persze elolvasás és kiértékelés után!) a bíróság gondolkodás nélkül visszadobja. Nem is kell nekik bizonyítékul, elég, ha támpontokat meríthetnek belőle, és az amerikai, a kanadai, az angol, az ausztrál és az új-zélandi kormányzat az Echelon és a Carnivore-programokon keresztül továbbra is alkotmánysértő módon hallgatja le – nem csak az állampolgáraik mobiltelefo-

nos és elektronikus kommunikációját. Valószínű, hogy az ön hangja is szerepel már valamelyik mappában elrejtve, dátummal, egy kódszámmal és minden szükséges adattal felcímkézve, viszont a legfontosabb dolgot mellőzve, mégpedig a beleegyezését igazoló nyilatkozatot.

A jogászoknak az Echelon-program okozza a legtöbb migrénes éjszakát, mivel a mobiltelefonok lehallgatására szakosodott műholdas hálózat, az ACLU elnöke szerint is, nem csak az ellenséges ügynökségeket figyeli: a békés civileket úgyszintén.

Az említett országok mind aktívan részt vettek a világméretű kommunikációs „elektromos porszívó" kifejlesztésében, és mára már politikai segédeszközként is használják az Echelont, amely képes felemelni bárkit a csillagos egekig, és arra is, hogy a mélybe taszítsa ugyanazt a személyt. De biztos, hogy szüksége van az emberiségnek erre?

A legtöbb szakmabeli, aki Amerikában tud az Echelonról és egyéb jelfogó megfigyelési technológiákról, kapcsolatban áll a nemzetbiztonságiakkal vagy bármely másik állami ügynökséggel, és ezek tanácsára nem feszegeti nagyon a témát. Az első komoly politikai fellépés az Európai Unió részéről történt, mely hatására elkezdték hivatalos szinten átvilágítani a rendszer működését.

De az erőfeszítések dacára pillanatnyilag semmilyen lehetőség nincs megvizsgálni, hogy az amerikai kormány milyen mértékben hatol az állampolgárok intim szférájába, mivel az adatvédelmi „kőtáblákba" vésett törvények nem szabályozzák az elektronikus kommunikációt. A mai kor technológiái jócskán (és tudatosan) meghaladták a ma is használt adatvédelmi törvényeket. Ezek újragondolása, megreformálása nélkül a kormányzat szabadon élhet és

visszaélhet jogaival. Szomorú, de az utóbbi az elterjedtebb.

Napjainkban követhetetlen, hogy az állami szervek, szakszolgálatok milyen mértékben élnek vissza technikailag korlátlan lehetőségeikkel. És később sem lesz arra lehetőségünk, hogy akár minimális szinten is, de belelássunk ebbe a körbe. Jó példa erre a „Közellenség" című film. Azoknak ajánlom figyelmébe ezt az alkotást, akik a könyvem sorait olvasva vizuálisan is át kívánják élni az általam leírtakat.

Egy kaliforniai vállalat azon fáradozik, hogy ingyenes szoftverükkel minél hamarabb hidegre tegyék az FBI e-mail-figyelő rendszerét. Elég bátor elgondolás. A NetworkICE 2004. szeptember elején hozta nyilvánosságra, a hírverést mellőzve, az Altivore nevű szoftverét, amely „alternatívát" nyújthat az adatfigyelésre kötelezett internetszolgáltatóknak a Carnivore-programmal szemben.

Ez a program képes mindarra, amit a Carnivore esetében felvázolt a kormány, azaz egy hálózat teljes adatforgalmából ki bírja szűrni a szöveges fájlokat, és keresni is tud bennük. A szoftver használható gyanús internetezők e-mailjeinek figyelésére (csak fejléc vagy teljes szöveg is kereshető), valamint figyelhető vele a gyanúsítottak teljes hálózati forgalma (web- vagy FTP-szerverekhez csatlakozás), a kimenő és bejövő adatforgalom lemásolható, és kinyomozható vele a szolgáltatótól kapott dinamikus IP-cím is.

Az FBI szakemberei a bejelentésre nem rémültek meg különösebben. Azt állítják, hogy már a kezdetektől fogva javasolják az internetszolgáltatóknak, hogy megfelelő szoftverekkel (de az ő belépési lehetőségükkel!) végezzék ők a megfigyeléseket. A Carnivore-rendszert csakis a szolgálta-

tók támogatására és védelmére hozták létre. Megható ez az „atyai gondoskodás", nem?

Az FBI megsejtette, hogy egy kétes hírű üzletember kifinomult titkosító technológia (Pretty Good Privacy-PGP) használatával tartja a börtönből (!) a kapcsolatot a külvilággal és az üzletfeleivel, így jó esély mutatkozott arra, hogy a leültetett gengsztervezér fiának a számítógépén esetleg megtalálják a sötét üzelmeik teljes adatbázisát. A profi nyomozók ezért egy olyan berendezéssel látták el a férfi komputerbillentyűzetét, amellyel minden leütést rögzíteni tudtak (keystroke recorder).

A készülék segítségével a gépből kinyertek mindent, amit lehetett. Ezzel az ügyes „trükkel" az FBI-nak nem kellett az internetszolgáltató szerverén elcsípni, majd iszonyatos erőművekkel feltörni a kódolt adatokat, hanem közvetlenül a főnök fiától értesültek mindenről. Ez a példa is jól illusztrálja, hogy van, akinek mindent szabad, van, aki meg csak nyel egyet. Én például nem vagyok bűnöző, viszont nekem is van számítógépem.

A vádlott védelmével megbízott ügyvéd szerint az FBI visszaélt egy házkutatási paranccsal, amikor 1999 tavaszán billentyűzetfigyelőt telepítettek ügyfele otthoni számítógépére. A május és június között összegyűlt információhalmazból a nyomozók kihámozták a titkosított dokumentumok kódolására használt jelszót.

Mivel a technológia gyorsabban fejlődik, mint ahogy azt a törvényhozás követni tudja, a nyomozók bármikor könnyűszerrel átléphetik az adatvédelmi aggályokat, arra hivatkozva, hogy amire nincs törvény, azt attól még lehet használni, és különben sincsen most idő arra, hogy kivárjanak egy döntést. Az ügyvéd szerint veszélyes és félelmetes, hogy a nyomozók mindent megszerezhetnek ügyfeléről, a neki írt, bizalmas leveleket, egészségügyi adatokat, törvényes üzleti információkat, kompromittáló szexoldalak jelszavait, egyszóval mindent.

Nem azért írom le már sokadszor azt a szót, hogy mindent, mert tetszik, hanem azért, mert sajnos ez az igazság. A mindenben meg benne van minden, ami körbevesz bennünket: én, te, ő, mi, ti, ők! Illetve vannak, akik nincsenek benne, mégpedig azok, akik uralják ezeket a rendszereket.

KEYLOGGERinctelenség

Billentyű-anatómia

Háromféle eszközzel lehet adatokat gyűjteni közvetlenül a billentyűzetről: egyrészt direkt erre készített szoftver telepítésével, másodsorban a billentyűzet és a számítógép közé iktatott kis csatlakozóval, és végül a billentyűzetbe rejthető egységgel.

Utóbbi a leghatékonyabb, mivel a kockacukor méretű, mindössze néhány gramm tömegű eszközt csak a rutinos billentyűzetemelgető felhasználók tudják kiszúrni. Az előbb említett bűnöző esetében használt készülék 32 millió leütést képes rögzíteni, amit a nyomozók vagy a telepítők a neten keresztül tudnak lehívni (beállítás szerint), néhány másodperces/perces késéssel. A figyelő monitoron ugyanazt látják, mint amit a célszemély a sajátján. Minden egyes billentyű leütését, a keletkezett parancsokat, műveleteket nyomon tudják követni. A keylogger hardvereszközök az adatvédelmi szakemberek és a számítógépet használók rémálma.

A keylogger szoftverek nem új keletűek, régóta léteznek, de a kiberbűnözés most kezdi igazán használni. A kereskedelmi alkalmazások és trójai behatolóprogramok (mint például a SubSeven, Back Orifice) egyaránt alkalmazzák az eljárást. A leütéslopók szoftveres változata a gépre menti a keylogot, vagyis az összes művelet másolatát, amit a program gazdája távlehívással bárhonnan, az interneten keresztül, be tud gyűjteni. Az ilyen, régóta ismert programok hátránya, hogy az operációs rendszer újratelepítésekor felülíródhatnak, vagy a hozzáértő felhasználók gyanút foghatnak, és a vírusirtókkal letörölhetik a behatolót.

A biztonságosnak tartott operációs rendszerek, mint például a Linux, a szoftveres leskelődést hatékonyan akadályozó védelmi rendszerrel vannak ellátva. A billentyűzetbe, vagy a billentyűzet és a gép közé kapcsolt keyloggerek azonban nem szorulnak rá az operációs rendszerre, a leütéseket a keletkezési helyükön jegyzik meg. Az ilyen eszközök kivédhetetlenek, és jelen pillanatban nincs is ellenszerük. Illetve egy van! Ha közelébe sem megyünk a számítógépnek.

Nem túlzok, ha azt állítom, hogy a lehallgatásra kifejlesztett és használt „poloskák" újabb generációjáról van szó, amelyek már a számítógépes adatforgalmat is teljes egészében képesek figyelni. A jelszavak, beléptető kódok és az adatállományok szám- vagy betűkóddal való védelme ilyen körülmények közt nem segít semmit. A támadó jellegű megfontolásokon túl persze néha jól jönne egy saját magunknak dolgozó keylogger is. Aki nem engedheti meg magának, hogy az összeomló szövegszerkesztőben elvesszenek az órákon keresztül gépelt szövegek, utolsó utáni mentésként felteheti a gépére a rendszertől független tárolóegységet. Az új-zélandi Keyghost Ltd egy ilyen hasonló rendszert kínál eladásra a piacon.

A Keyghost (Szellemkulcs) névre hallgató terméknek számos változata van. A Standard és a Professional változat hengeres házat kapott, amelybe kétoldalt a billentyűzet adaptere csatlakozik. A telepítés mindössze annyiból áll, hogy a készüléket a tasztatúra csatlakozója és a gép PS/2 portja közé kell illeszteni. A kábelbe iktatott eszköz hátránya, hogy egy megfigyelni kívánt idegen gép tulajdonosa könnyen felfedezheti.

A Standard változat 97 ezer karaktert tud megjegyezni. A Professional II.-es széria már félmillió, a Professional II.

SE pedig kétmillió billentyűleütést tárol el. A rögzített adatokat ezenkívül a professzionális változat 128 bites titkosítással is védi. A készüléket akár egymás után több gépre is fel lehet csatlakoztatni, és az adatok kiolvasására bármilyen szövegszerkesztő alkalmas.

A laikusnak fel sem tűnik, hogy milyen csatlakozásokkal kapcsolódnak a részegységek egymáshoz. Ha eleve olyan gépet vásárol, amihez már csatlakoztatva vannak ezek a „szellemkulcsok", akkor hozzájuk sem mer nyúlni, mert úgy gondolja, hogy ezek tartozékai a teljes konfigurációnak.

A fenti problémát és a feltűnést kerüli a már piacra dobott Security Keyboard. Ennél az eszköznél a szerkezetet a hagyományos billentyűzet belsejébe építik be. Az EU-ban a hasonló szaglászó hardvereszközök használatát alig korlátozzák szabályok, ezért itt igen elterjedtek. Egy ilyen klaviatúrát 5 másodperc alatt ki lehet cserélni egy irodában vagy egy lakásban.

A magánszférát és a személyes adatokat védő rendelkezések szellemében például csúnya dolognak minősül egy ilyen eszközt csatlakoztatni másnak a gépére. Ez így van! De ez senkit nem érdekel a túloldalon! Egy vállalat csak a munkatársak hozzájárulásával ellenőrizheti a szörfölési szokásokat. Ez a hivatali megközelítés, a privát pedig az, hogy házon belül bármit csinálhatnak.

Az biztos, hogy sok esetben nem az ár az, ami visszatartja a vezetőket a szerkezetek telepítésétől, mivel a legprofibb sem kerül többe kétszáz-háromszáz dollárnál. A hírnevük csorbulása inkább visszatartó erő. Ha az a hír terjed el róluk, hogy még a WC is be van poloskázva, akkor senkinek nem lesz kedve ott dolgozni, és lehúzhatják a rolót. Mert ki szeretne olyan helyen dolgozni, ahol minden mozdulatát és sóhajtását figyeli valami vagy valaki?

JELSZÓrakozás

Mondd meg, ha tudod!

A legfontosabbal kezdem: a jelszó védelme annak a kitalálásával kezdődik. Nem a megfejtésével, hanem a megalkotásával. Az emberek többsége hajlamos egyszerű – évszámhoz, becenévhez kötődő – jelszót gyártani, illetve elkövetni a hibák hibáját, hogy minden egyes programhoz, az internetlevelezéshez és a fórumokhoz ugyanazt a jelszót használja.

A leggyakoribb hiba, hogy jelszónak a felhasználónevet adják meg, netán egy számjeggyel megtoldva a végén. Ne feledjük el, hogy az előfizetéshez adott jelszó egyszerre az internetes postaládák kulcsa is, fel tudunk vele lépni az internetre, és átírhatjuk vele a saját készítésű weblapunkat is!

A másik ilyen csapda a kényelmesség. Milyen könnyű is egy gombnyomásra betárcsázni a szolgáltatóhoz, vagy rábízni az Internet Explorer-re a jelszavak megjegyzését! Ezt soha ne tegyék, mert ezek a hozzáférési adatok minden esetben rögzítődnek a gépen, jól-rosszul elrejtve és kódolva.

Aki rossz szándékkal, a hálózaton keresztül vagy fizikailag hozzáfér a géphez, könnyen lenyúlhat minden elmentett jelszót. Ők tudják, hogy hol kell keresni azokat. Az észbe vésésre váró jelszót sokszor szótári (vagy ahhoz közel álló) formában adják meg. Szintén szarvashiba!

Az angol nyelv standard karaktereiből álló 6 betűs jelszó (általában ennyit kérnek a különböző szolgáltatók!) ilyen körülmények közt egy alig 32 bites titkosítási kulcsnak felel meg, amit már feltörhet bárki az interneten elérhető és letölthető feltörő programokkal. A 128 bites titko-

sítási szintet egy 96 karakteres szöveggel való védelem jelenthetné. Ez már igen! Csak ki tud megjegyezni egy 96 karakterből álló jelszót? Szerintem senki.

A legtöbb jelszótörő program az angol nyelv szótárával indít, de nem lehetünk biztonságban egyik nyelv leírt szavának szótári alakjával sem, mert a jelenlegi fejlett technika már csak ilyen!

Meg lehet próbálkozni az egyre bonyolultabb jelszavak alkalmazásával, bár a határokat is látni kell. Azt senkitől nem lehet elvárni, hogy megjegyezzen egy (vagy több) 32 karakteres hexadecimális sort. Minden jó jelszót nehéz megjegyezni, de épp ettől lehet remélni a biztonságot alapesetben, például keyloggerek nélkül. Ha ilyen van a gépünkön, kitalálhatunk bármilyen bonyolult jelszót, mert abban a pillanatban, amikor ráütünk a billentyűkre, már nem is titok többé.

Mindenkinek magának kell kitalálnia a jelszavát, ne fogadjunk el senkitől tippeket! Fura kinézetük ellenére használhatónak bizonyulhatnak a szolgáltatóinktól kapott, vagy ahhoz hasonló, elméletileg véletlenszerűen generált jelszavak. Kisbetűk, nagybetűk, speciális karakterek (ékezetes betűk kivételével), nem könnyűek, de legalább biztonságosabbak. Ha a jelszavunkra költünk egy mondatot, úgy már jól meg tudjuk jegyezni. Egy példa: VvlaFr14 = Vive la France, és a Bastille ostromának napja, július 14.

KÓDOLIár

Kódorgás

A tökéletes titkosítás egyszerre áldás és átok egy titkosszolgálat számára. Ezért is építenek hátsó kapukat a kereskedelmi forgalomba kerülő titkosító eszközökbe. Úgy nem is kerülhet hivatalosan eszköz a piacra, hogy ne engedélyeznék a szolgálatok annak működését. Az engedélyezés pedig hátsó kapuk nyitásával jár.

Ez igen veszélyes helyzeteket teremthet. A hátsó kapuk nélküli titkosító algoritmusok által generált kódot egyéb támpontok híján csak a nyers erővel (az összes lehetséges kulcs felhasználásával) lehet visszafejteni. Ez bizony időbe telik. Méghozzá nagyon sokba. Hogy mennyibe is valójában? Ez jelenleg leginkább a számítógépek műveleti sebességétől és a kulcshossztól függ. Egy gép esetén néhány száztól néhány százmilliárd évig terjedhet az időigény. Valamivel jobb a helyzet, ha több számítógép dolgozik egyszerre a feladaton.

Évek óta folyik egy verseny kódtörő csapatok között az RSA Labs különféle hosszúságú kulcsainak megfejtésére. 1997-ben 250 nap alatt feltörték az RSA Labs 56 bit hosszúságú kódját. A sikeren felbuzdulva még abban az évben elkezdték a csapatok a 64 bites változat visszafejtését. A több mint 4 évig tartó erőfeszítést siker koronázta.

Négy év alatt a 18.446.744.073.709.551.615 (kimondani sem tudom) lehetőség közül 12.267.884.765.079.666.688 különböző kulcsot, vagyis a feltöréshez szükséges mennyiség mintegy 67%-át sikerült végigpróbálgatni. A munka kezdete óta eltelt idő alatt azonban megsokszorozódott

a visszafejtést szervező Distributed.net rendelkezésére álló számítási teljesítmény.

A növekedés oka kettős. Egyfelől a részt vevő gépek száma, másrészt azok teljesítménye is növekedett. A statisztikák szerint a számítási teljesítmény 261 naponta megduplázódik. A növekvő kapacitással magyarázható, hogy míg a lehetséges kulcsok 67%-ához 1541 napra, addig a maradék 33%-hoz csak 339 napra volt szükség. A 64 bites RC5-64 kód feltörése az eddigi legnagyobb ilyen jellegű vállalkozás.

A munkában jelenleg több mint 315 ezer önkéntes, több mint 12 ezer csapatba szerveződve vesz részt. Ez pillanatnyilag a gépek számát és sebességét figyelembe véve összesen 92.141.082.000 kulcs/s fejtési kapacitás. A legsikeresebb csapat neve Dutch Power Cows. A közeli siker után még kérdéses, hogy nekifog-e a Distributed.net a 128 bit kulcshosszúságú kód megfejtéséhez, hiszen a mai számítási teljesítményeket figyelembe véve ennek a kódnak a megfejtéséhez mintegy 117.106.103.342.763.157.348 évre volna szükség...

Láttak már bizonyára olyan fotót, amin egy szakállas ember (aki történetesen a legrettegettebb és legkeresettebb muszlim terroristavezér) előszobaszőnyegbe tekeredve AK-47-essel a kezében álldogál a kietlen afganisztáni puszta közepén. Elég furcsán hangzik, de ő az a személy, akit még mindig keresnek a világ legprofibb hírszerzői és ügynökei. Hogy miért nem tudták még elfogni?

Vagy azért, mert többet tud, mint az összes szolgálat egybevéve, vagy a jobbik esetben már nem is él, csak a neve és a mesterségesen fönntartott szelleme. A Hamasz, a Hezbollah és bin Laden csoportjai igen kifinomult, és rendkívül képzett embereket is alkalmaznak. Felszereltségük kitűnő, és rendkívül profi szakemberek dolgoznak velük. Ezek az emberek vagy fanatikusak, vagy az életükért és a családjuk életéért dolgoznak a terroristáknak.

Az FBI-nak folyamatosan fejfájást okoz a titkosítás. 1999 ősze óta szabadon exportálhatók az Egyesült Államokból az erős titkosításra képes programok. Az is igaz, hogy egy törvény vagy exportkorlátozás semmit sem akadályozna meg: a terroristák és a bűnözők nem a boltban vásárolják meg a titkosító szoftvereket és berendezéseket. Ráadásul Európában, Ázsiában és a Közel-Keleten is tudnak programokat íratni. Az FBI igazgatója szerint a terroristacsoportok 1996 óta használják az elektronikus titkosítást. A nyomozó hivatal ezért mindenképpen szeretne hozzájutni a használatban lévő programok mesterkulcsaihoz, és ez által hozzáférni az emberiség számára veszélyes, gonosz tervekhez.

A bűnüldöző szervek azért mégsem teljesen tehetetlenek a terroristákkal szemben. Az amerikai felderítés kódtörő szakosztálya elért már szép sikereket a lekódolt és levajazott terrorakciók megakadályozásában. A kelet-afrikai amerikai követségek ellen elkövetett merényleteket ugyan nem sikerült megakadályozniuk, viszont az e-mailek megfigyelése és dekódolása alapján az egyik elkövető, Wahid El Hage már bíróság előtt áll.

A pakisztáni Khali Deek jordániai bombatámadásokat tervezett, de már nem tudott pusztítást okozni, mert 1999-ben elfogták. Számítógépét a peshawari, kis alapterületű, szoba-konyhás lakásából az NSA Fort-Meade központjába repítették, ahol a szuperkomputerek sikeresen feltörték a tervek kódolását.

A World Trade Center elleni 1993-as első bombatámadást kitervelő Juszuf Ramzi szintén lebukott. Hardverét 1995-

ben foglalták le a Fülöp-szigeteki hatóságok. Ramzi akkor tizenegy amerikai repülőjárat felrobbantásának tervén dolgozott éppen. A szakemberek elmondták, hogy két olyan fájl is volt a gépen, amelyek feltörése több mint egy évet vett igénybe.

A „szent háború", a dzsihád során elesetteknek a „Paradicsom" kéjekkel teljes kertjét, a meghátrálóknak és gyáváknak a „Gyehenna" kínjait ígéri a Korán.

Az iszlám hackeretikát ennek szellemében úgy módosították egy nemrég üzembe helyezett fundamentalista szerver szoftverbázisán, hogy az iszlám harcosoknak belépés előtt el kell fogadniuk az „esküszöm, hogy kizárólag zsidók és izraeliek ellen használom az innen letölthető programokat" figyelmeztetést. A számítógépes fegyverarzenálban hacker-segédprogramok, vírusok és makrovírusok széles választéka szerepel, és a szokványos gyilkoló repertoár. Ám a „csodafegyvert" itt is az elkeseredés, és a megfélemlítő gyilkos, vagy éppen öngyilkos ideológia pótolja.

Az Egyesült Királyság rendfenntartó szervei a 2000 júliusa óta hatályos RIPA (Regulation of Investigatory Powers Act, nyomozati jogkörökről szóló törvény) értelmében bőségesen átnézhették bárki elektronikus leveleit, informálódhattak egészségi állapotáról, szexuális szokásairól, vallásos meggyőződéséről, filozófiai és politikai világképéről és ismeretségeiről az internetszolgáltatóknál törvényileg kötelező poloskatelepítési programot követően. Ezt csak azzal a felhasználóval nem tehették meg, aki hazafiatlan módon titkosító szoftvereket használt.

Ezt azzal a törvénnyel egészítették ki 2002 folyamán, amely a RIPA harmadik bekezdésének végrehajtását biztosítja, miszerint kötelezővé tették a kriptográfiai progra-

mokat használó felhasználókat, hogy adják át titkosító kulcsukat a hatóságoknak; aki ezt nem teszi meg, és jogtalanul használ ilyen programokat, arra vár a börtön.

Mint látható, a védelmi szervek kezdenek bekeményíteni, mivel a jövőjük nagyban függ attól, hogy mennyire lesznek képesek megfékezni az ellenőrizetlen titkosító szoftverek és algoritmusok elterjedését.

AUTOMATIKAland

Embertelenség

A mobiltelefonokhoz hasonlóan a jövőben akár autónkat is megfertőzheti egy „járvány", így nem kizárt, hogy ezen védelmekre kocsinknak is szüksége lesz. A világ legnagyobb vállalatainak biztonsági tanácsadó divíziói nemrégiben elkészítettek egy jelentést, melyben a jövő digitális világának fenyegetéseit vették számba. Eszerint olyan veszélyhelyzetek leselkednek ránk, melyeket azért a felkészült emberek képesek ellenőrzésük alatt tartani. Ezt én is szívből remélem.

De ha belegondolunk abba, hogy eddig még nem hallottunk olyan hírt (legalábbis én nem hallottam!), hogy egy még nem aktivált, kegyetlen vírust a pusztítása előtt hatástalanítottak volna, akkor ez az előbbi kijelentés nagyképűségnek hangzik. Mi az, hogy képesek ellenőrzésük alatt tartani?! És mit? Azt sem tudják, hogy mi várható, vagy hogy milyen támadásra készüljenek fel.

Ha nem ismerik a támadót, hogyan védekezhetnek ellene? Hogyan tudnának egy vakcinát kifejleszteni, ha nem ismerik a törzset, és nincsen meg a hordozó sem, amely az ellenszérumot ki tudná termelni részükre? És ráadásul ehhez a kijelentéshez számos nagy üzleti felhasználót kérdeztek ki, kormányzati biztonsági statisztikák és vizsgálatok adatait összesítették, melynek eredményeként a több ezer konzultáns a fenti megállapításra jutott.

Mint már tavaly is tapasztalhattuk (szerencsére legtöbbünk még csak a beszámolók alapján), a férgek és vírusok „kiköltöztek" a számítógépről: megtalálták maguknak a mobiltelefonokat és a tenyérgépeket, melyeket eddig nem fenyegettek. A vezetékmentes hálózatok és a beágyazott rendszerek – az egységesítésre való törekvésnek köszönhetően – is egyre inkább veszélynek vannak kitéve. Ezek szerint azok is haladnak a divattal és az igényekkel. Most ezek a slágerek, ezért jó célpontok is egyben.

A 2004 végén készített „Security Threats and Attack Trends Report" nevű jelentés mindezt továbbgondolva arra a következtetésre jutott, hogy előbb-utóbb a személygépkocsik is érintetté válnak, ahogy minél több elektronikával látják el őket a gyártók. A biztonsági stratégiákért felelős igazgató egy interjú során azt fejtegette, hogy az autókat a számítógépekhez hasonló fenyegetések veszélyeztetik, némelyik direkt rossz szándékkal okozhat majd bajt, míg más problémák akaratlanul, nem előre kitervelt módon bukkannak fel.

Egy átlagos autó 10–20 processzorral és több tíz megabyte-nyi szoftverkóddal rendelkezik, olyan, mint egy komputer, ezért felmerülhet az ilyen meghibásodások valószínűsége, nem szólva a biztonsági rések vezetékmentes kapcsolaton keresztüli kihasználásáról. A jövőben tehát nincsen kizárva, hogy nem csak otthoni számítógépünkre kell vírusvédelmi szoftvereket telepíteni, hanem a mindent tudó autóink fedélzeti komputereibe is.

Erről is született már egy vicc: Az új 7-es BMW-be beleszalad hátulról egy Mini Morris. A BMW fedélzeti komputerén a következő felirat jelenik meg: „Új Plug&Play eszköz csatlakozva. Telepíti most a szükséges drivereket?"

A vezeték nélküli chipek célja a jármű indításgátlása, amennyiben nem a megfelelő kulcsot használják. Tavaly körülbelül 150 millió ilyen chipet dobtak piacra, melyek többsége használatban is van. Avi Rubin, a számítógép-tu-

dományok professzorának csapata azt a technikát alkalmazta, amivel a hackerek a rádiófrekvencia-azonosítási (RFID) chipeket törik fel.

A kutatók által ostrom alá vett rendszer két részből állt. Egy, a kulcsba ültetett átjátszó chip, valamint egy olvasó az autó belsejében, ami az üzemanyag-befecskendező rendszerrel van összeköttetésben. Ha az autó olvasója nem ismeri fel a kulcs chipjét, az autó nem indul el akkor sem, ha a kulcs amúgy illik az indítóba. Az olvasó egy ún. feladat-reakció protokollon keresztül ismeri fel a kulcsot. Amikor az autó kulcsa a közelben van, az olvasó egy nullákból és egyesekből álló, véletlenszerű adatláncot sugároz, amit a kulcs chipje feldolgoz. Ezután a chip hitelesítésként egy numerikus üzenetet küld vissza az olvasónak.

A gond ezzel a rendszerrel az, hogy az autó nem a tulajdonosát ismeri fel, hanem a kulcsba épített chip által generált kódot, és a kulcs akár egy tolvaj kezében is lehet.

A kutatók ebbe a folyamatba ártották bele magukat azáltal, hogy megfejtették az ellenőrzéshez alkalmazott matematikai folyamatot, ami lehetővé tette számukra, hogy kiiktassák az autó lopásgátló rendszerét úgy, hogy a biztonsági chipnek nem is kell jelen lennie a gépjármű elindításához. Na tessék, ez az ötlet sem jött össze! A szakértők nem változtattak a rendszer biztonságán, csupán egy gyengeségét hozták a napvilágra. Úgy gondolják, ha nem a tudósok találják meg a rendszer gyengeségeit, akkor előbb-utóbb megteszik helyettük a bűnözők, akik ezt könyörtelenül ki is fogják használni. Ezzel pedig mindannyian egyetértünk!

Az igazsághoz mindenesetre hozzátartozik még, amit a kutatók is elismernek, hogy az indításgátló rendszerek nem kevesebb mint 90%-kal csökkentették az autólopások számát, valamint azt is tudni kell, hogy a távirányítós rendszerek, melyekkel nyithatók-zárhatók a gépjárművek, nem alkalmaznak RFID-chipeket.

De sebaj, kitaláltak mást, mégpedig egy iltag (intelligent license tag) nevű, kártyalap méretű matricát, amelyet a szélvédő belső felére kell felragasztani. Az autólopás ellen nincs biztos védelem (amelyiket el akarják vinni, azt el is viszik), mégis a technikának köszönhetően megnehezíthető a tolvajok dolga. A matricába egy chip van beleépítve, amelyet csak különleges berendezésekkel lehet leolvasni. Az új német fejlesztés nem a lopást gátolja meg, hanem az újraértékesítést.

A matrica védelme kettős. A felületére jól olvashatóan felkerül a jármű rendszáma, a beépített chipbe meg az autó tulajdonosának adatai, biztosítási információk, a jármű vezetésére jogosult személy(ek) neve. A tárolt adatokat csak speciális dekódoló berendezéssel lehet kiolvasni és megváltoztatni. A chip nagyon érzékeny, így gyakorlatilag lehetetlen sérülésmentesen eltávolítani. A technológia kifejlesztésében három cég: az Infineon (a chipet gyártja), a Schreiner Prosecure (a hologramos védőfóliát gyártja) és az Utsch vett részt. A chipet lassan mozgó járműből is le lehet olvasni, így a rendőröknek is könnyebb a dolguk.

DEMOKRATAkarítás

Szeressük egymást...!

A demokrácia csapdája is veszélyes lehet. Több amerikai államban akarták az iskolákban felállítani a szoftveres szűrőket, hogy az internet adott helyen szükségtelen részeit – pedofília, pornográfia, erőszak stb. – kizárják.

A demokratikus jogokért síkra szálló szülők azonban megnyerték a pereket: az amerikai iskolákban semmifajta szűrést nem lehet alkalmazni, mert az sértené a demokratikus jogokat. Ki szereti az olyan általánosításokat, mint ez, de vannak dolgok, amiket nem lehet általánosan (törvénnyel) elintézni. Bár kényelmesnek tűnik, de lehetetlen. Van, amihez egyedi, aprólékos, manuális hozzáállás kell.

Ez ismét egy abszurd és morbid húzás. A szülők hagyják, hogy a gyerekük felügyelet nélkül látogassa az internet szennyes oldalait, közben meg csodálkoznak, amikor előjön az agresszivitás belőlük. És csak annyit mondanak egy-egy sajnálatos eset után, hogy ki gondolta volna erről a gyerekről, hogy képes megtenni ilyen szörnyűséget...

Ismerik a viccet a borbélyautomatáról? Felállítják egy moszkvai aluljáróban a borotváló automatát. Ivan Ivanovics körüljárja, megszemléli, és fejcsóválva azt mondja Nyikolaj Nyikolajevicsnek:

– Szerintem ez használhatatlan! Ki az az őrült, aki bele akarna ülni? Hiszen minden embernek eltérő a fizimiskája!

Nyikolaj Nyikolajevics mosolyogva válaszol:

– De csak az első használatig!

Ha belekényszerítenek bennünket, akkor valóban egy fazonra leszünk nyírva. Ez igaz az informatikára, persze akkor könnyebb lesz a... és nehezebb lesz a... és az ötlet átvihető a gondolati piacra, a szoftverpiacra, és bárhova. A rendszergazdáknak természetesen egyszerűbb a rendszer biztonságát megtervezni és megvalósítani, ha minden felhasználó azonos gépet, azonos operációs rendszert, azonos beállítást használ. Ezzel viszont a támadók helyzetét könnyítjük meg.

Annak idején magabiztosan jelentették ki a szakemberek, hogy nincsen olyan vírus (kártevő), ami a különböző operációs rendszereken egyaránt életképes. Ezért aztán létrehoztak egy közös felületet (Virtual Machine), ami minden rendszer alatt hasonlóan sebezhető az azonos tulajdonságok (és hibák) miatt.

Így lehetséges az, hogy a HTML, Java, Javascript stb. kódok minden rendszeren bajt okozhatnak. Tehát rúgtak egy nagy öngólt, és a labda még mindig a hálóban van. Ki kellene venni, és jó messzire elrúgni!

HACKERkölcstelenség

Töréstesztek

Bármilyen titkosítást, amit egy ember kitalál, azt egy másik ember meg tudja fejteni. Elvileg! Gyakorlatilag ez csak akkor derül ki, ha valóban meg is teszi. Becslések szerint egy-egy érdekesebb szervert naponta 100-150 hacker próbál feltörni, nem csoda hát, hogy időnként valakinek sikerül is. Ez az, amiről az átlagembernek fogalma sincs: aki még a Worddel is nehezen birkózik, el sem tudja képzelni, mi is az, hogy feltörni...

A hackertársadalom csúcsát a valódi hackerek képviselik. Ők tényleg a professzorai a gépeknek, belőlük kerülnek ki a rendszergazdák, rendszerszervezők, és a fizetésük súrolja a csillagos eget. Éppen ezért a legritkább esetben követnek el bűncselekményeket. Ők az élharcosai azoknak, akiknek az internet biztonsága mindennél fontosabb. Vigyáznak is rá kegyetlenül! Lecsapnak azokra, akik megszegik az írott és íratlan törvényeket. Teszik ezt azért, mert tisztában vannak azzal, hogyha meginog a multik bizalma a világhálóban, azzal közvetve a saját megélhetési forrásaik is veszélybe kerülnek!

Soha nem pihennek, éjjel-nappal résen vannak, és keresik a biztonsági rendszerek hibáit a megbízást adó cégeknél. Ha be tudnak hatolni a célterületre, akkor már meg is találták, és nyomban intézkednek az adott hiba elhárításáról. Tevékenységüket sokan misztifikálják, de ők is emberek, és legfeljebb szaktudásuk elismerésre méltó. Én is ismerek ilyen embereket, szívesen vagyok a társaságukban, sőt dolgozom velük együtt.

A többség a kormányhivataloknak és szolgálatoknak dolgozik, természetesen fedésben. Olyan információk birtokában vannak, amit csak kevesen ismerhetnek meg. Munkájuk és életük nem éppen stresszmentes, de ők ezt választották. Ha jó és nemes célról van szó, akkor önzetlenül segítenek, ám ha be akarják húzni őket a csőbe, akkor méltó és kemény ellenféllé válnak. Híres a titoktartásuk. Mindig a megbízók érdekeit tartják szem előtt, és ritkaság, ha két vagy több irányba dolgoznak.

A light-hackerek tábora sokkal népesebb az előzőnél. Ők nagyságrendekkel szerényebben élnek, megspórolt pénzüket gépeik fejlesztésére költik. A többségük egyetemista, akiknek az informatika jelenti az életet. Minden vágyuk, hogy bekerülhessenek a csúcskategóriások közé. Erejüket és tudásukat próbálgatva keresik a támadható felületeket a hálón. Gyakorlatilag semmiféle hasznosat nem csinálnak, hobbi tevékenységük abban merül ki, hogy betörnek egy weboldalra vagy szerverre, és arra mindenféle idétlen dolgot felraknak.

Néhányan közülük azzal váltak híressé az Államokban, hogy az FBI honlapjából egy pornográf lapot kreáltak. Sokak örömére, és az FBI szégyenére. Ezt hívják image-rombolásnak. Természetesen pillanatokon belül elkapták őket, mert az ellenoldalnak is dolgoznak az előző táborban tevékenykedő profik, akik nem szeretik, ha valaki beleüti az orrát a nagyok dolgába.

A dark-hacker (vagy evil) bűnöző. Nyereség- vagy bosszúvágyból végzi tevékenységét, kémkedik, illetve mások által fizetett hitelrontásból él. Ő csapolja meg az ön bankszámláját, ő teszi közzé az ön cégének adatait, ő készíti az internetes vírusokat, ő formázza le a távolból az ön winchesterét. Önnek ő a legnagyobb ellensége.

A sötétség vándora, aki az éjszaka leple alatt lopódzik be áldozata életébe, még az álmaiba is. Kegyetlenül, élve zsigereli ki, akit csak lehet. Nincs benne könyörület. Az anonimitás álarcában végzi nem éppen áldásos tevékenységét. A bosszúállás az egyik lételeme, a másik pedig a pénz. Az, hogy mit okoz embertársainak, az emberi érzések abszolút hidegen hagyják. Nem kívánom senkinek, hogy egyszer egy ilyen hiéna támadását kelljen átélnie.

Külön kasztban élnek a phreak-ek, akik a telefonközpontok vezérlő-számítógépeinek, a távközlési vonalak ingyenes igénybevételének, és általában a telekommunikációnak a szakértői. Rendelkeznek a központok átprogramozásához szükséges tudással, illetve megfelelő eszközökkel a mobiltelefon-hálózat forgalmának, belső adatainak lehallgatásához. Ők egyfajta parazita életet élnek, másokon élősködve végzik a munkájukat.

Az okozott kár az NSA 95-ben kiadott adatai szerint már akkor több mint 4 milliárd USD volt, azóta a technika még fejlettebb lett ezen a területen is. Nem nehéz elképzelni, hogy ez a szám jelenleg mekkora lehet, ha tisztában vagyunk az eltelt 10 év alatt történt technikai változásokkal és fejlesztésekkel. Olyan mobil eszközökkel rendelkeznek, hogy a világ bármely pontjáról képesek pillanatok alatt bárkit elérni, és a kommunikációs rendszerét maximálisan kihasználni.

A wannabe-hacker, mint a neve is mutatja, nem valódi hacker, csak szeretne az lenni. Ő az, aki legjobban hangoztatja, hogy mivel foglalkozik. Próbál a nagyok nyomában járni, de sokszor tudatlanságával és tapasztalatlanságával több kárt okoz még a profik jó hírének is, akik próbálják kontrollálni a tevékenységüket.

Ha esetleg olyan helyen bóklászik, ami már foglalt, akkor blokkolják a tevékenységét. Egyszer-kétszer még próbálkozik, de aztán rájön saját maga is, hogy még sokat kell tanulnia, ha ebből a szakmából akar megélni. Képtelen arra, hogy önálló programokat írjon, ezért a mások által kitalált hack-programokkal, exploitokkal dolgozik. Az ilyenekkel el van árasztva az internet. Ezek a programok sok esetben csapdák, és a szolgálatok szakemberei találják ki őket, akik le akarják buktatni a kezdő hackereket. Ezzel a módszerrel be tudják juttatni saját figyelő programjaikat az ellenséges gépekbe. Utána folyamatosan tudják figyelni a tevékenységüket, és a megfelelő időben beavatkozhatnak. A hackerek munkájának kontrollálásával sok információt össze tudnak gyűjteni, erőfeszítés nélkül.

A legfiatalabb réteget a trollok (a mesékből ismert, gonosz manók) alkotják. A trollok előképzettség nélkül gyakorlatilag céltalanul ténferegnek a világhálón, és tönkretesznek minden elébük kerülő és támadható dolgot a neten. Mivel nem tudatos a tevékenységük, így a szokásaik ismerete nélkül nehéz követni a rombolásukat.

Hasonlítanak a wannabekhoz, mert ők is konzerv programokkal dolgoznak, azonban az előbbiekkel ellentétben rendszerint fogalmuk sincs arról, hogy mit csinálnak. Büntethetőségük a koruk miatt általában nem lehetséges.

A drifterek viszonylag a legártalmatlanabb figurák. Ők csak keresnek valamit, megtalálják az ön gépén, lemásolják maguknak és továbbállnak. Akkor van probléma, ha az a valami pont egy titkos információ. Tevékenységük rendszerint észrevétlen marad, legfeljebb a modem folyamatosan, de minden ok nélkül villogó transmitted led-je utal jelenlétükre.

Sokféle hacker van tehát. A köznyelv keveri is az önérzetes hackereket a sokkal agresszívebb crackerek csapatával, noha egyszerű a megkülönböztetésük. Nézzük sorjában:

A cracker feltör, a hacker betör. A cracker minden esetben jogot sért, és ezért bűnöző, az igazi hacker megbecsült munkaerő. A cracker előre megfontolt szándékkal károsítja meg a szoftvergyártót, hackelni lehet szinte véletlenül is.

A cracker a saját gépén lévő anyagot okosítja meg, míg a hacker egy távoli számítógépet cserkel be. A cracker hangos, dicsekszik, a hacker csöndben van és bölcs.

A cracker tevékenységével lojálisabbak az emberek, sőt van, aki örül neki a sok olcsó kalózmásolat miatt, a hacker ellenben a XXI. század fő kereskedelmi formáját, az e-businesst veszélyezteti, tehát közutálatnak örvend ebben a körben. A cracker által okozott kár igazán csak a szoftvergyártónak érdekes, tehát a kár inkább relatív jellegű, a hacker által okozott kár viszont azonnal zsebre megy (például ha megtudja a bankkártya adatait).

A crackerek különböző operációs rendszerekre és platformokra specializálódtak. Próbálgatnak, kísérleteznek, amíg valami „használhatóra" nem bukkannak. Márpedig ez nem nehéz, mivel a jelenlegi szoftverek és operációs rendszerek komoly mennyiségű problémával, támadható felülettel rendelkeznek.

Sokszor azon csodálkozom, ezek ismeretében, hogy a gyártók milyen jogon vetetik meg velünk ezt a sok szemetet. A legszomorúbb az a tudat, hogy ezt meg is fogják tenni egészen addig, amíg a felhasználók össze nem fognak ellenük, és nem bojkottálják a tevékenységüket. De a vélemények megoszlanak, ezért nehéz érvényesíteni ellenük bármit is. A kártérítési perek összegét zsebből kifizetik.

A támadások első lépéseiben a cél mindig az interaktív kapcsolat (login) megszerzése, ami kemény munkával továbbfejleszthető root vagy superuser jogkörré, aki egy-egy gép legfőbb adminisztrátora, vagyis elsődleges irányítója.

A drága szoftvereknek általában kiadják a legyengített, lebutított verzióját, ingyen, kipróbálás céljából. Ezeket a „nyalókákat" hívják light vagy trial verzióknak, evaluation copy-nak, special edition-nak. Az ok nyilvánvaló: aki ezeket kipróbálja, előbb-utóbb nem tud meglenni nélkülük, tehát megveszi őket. Muszáj, mert a butított verzió néhány nap után leáll, vagy a legfontosabb funkciókat nem hajtja végre, így vannak kitalálva. Ha például a verziókat használva állít össze valaki egy dokumentumot, a határidő lejárta után nem tud hozzáférni. Ebben a fázisban lép a színre a cracker, többféle módon:

Patch-csel, vagyis a megfelelő dekóder-programmal visszafejti a szoftvert, és megkeresi azt a rutint, amelyik a határidő-számlálásért felelős. Ezután ír egy programot, amely kivágja a megfelelő részt az eredeti szoftverből úgy, hogy a többi funkció ne sérüljön. Ez a patch, amelyet aztán jó pénzért el lehet adni másoknak, illetve ki lehet tenni a netre, „emberbaráti" célokból, hogy más hozzá nem értő személy, azaz a lamer (béna) is meg tudja operálni a saját szoftverét.

A kódtörő programokkal egyszerűen feltöri a passwordot (jelszót). Minden szoftver a határidő letelte után kéri az azonosító jelszavát. Ezt a gyártó/forgalmazó küldi meg a felhasználónak, miután valaki kifizette a szoftver árát. Na már most a cracker abból indul ki, hogy a szoftvernek eleve ismernie kell a jelszót ahhoz, hogy azonosítani tudja. Ha pedig a jelszó ott van a fájlban, akkor azt meg is lehet találni. Zsigereire szedi a programot, minden gyanús karaktersorozatot kipróbál, és addig próbálkozik, amíg az egyik működni fog. A jelszóval meg oda telepíti a programot, ahová akarja.

De sok esetben kulcsgenerátort (KeyGen) használ. Ez a legelegánsabb megoldás. A jelszavakat ugyanis egyes szoft-

verek úgy állítják elő, hogy a beírt felhasználónév betűinek kódját bizonyos matematikai művelet szerint átszámolják, és a kapott karaktersorozat a jelszó. A filmekben látni ilyet, amikor az ügynökök, vagy éppen a rossz fiúk, ott állnak egy kóddal zárt, önműködő ajtó előtt, és rácsatlakoznak egy ügyes szerkezettel a beléptető rendszerre. Majd láthatjuk, hogy egy sok számból álló számsor félelmetes sebességgel pörögni kezd, és egymás után állnak meg a számok a kijelzőn, a végén pedig kattan a zár és kinyílik az ajtó.

A cracker ezt a programrészt találja meg, ezt kivágva és önálló életre keltve bármilyen névhez megtalálható a jelszó. A lamernek (tudják, a komputer-analfabétának) általában ez tetszik a legjobban, hiszen a szoftver így az ő nevére lesz regisztrálva, legalábbis látszólag. Emlékeznek még arra, amikor azt írtam, hogy ebben a műfajban semmi és senki nem az, akinek és aminek látszik? Éppen ez benne az izgalmas, és egyben a veszélyes is. Soha ne felejtsék el, hogy akik ilyen alantas tevékenységet folytatnak, azok nem azért teszik, hogy jótékonykodjanak, hanem azért, hogy maguknak valamilyen formában hasznot hozzanak.

Tehát például, ha egy kalózszoftvert kap ajándékba, aminek nem tudhatja az eredetét, lehet, hogy pont a számítógépének zombivá válását indítja el önként és dalolva. Pedig, ha tudná, akkor messzi ívben elkerülné még azt is, aki ezt ajánlja önnek. De sajnos az emberek többsége nem így gondolkodik, a vírus meg csak terjed és terjed megállíthatatlanul.

A hálózatba kötött számítógépek elvileg egymás bármely fájljához hozzáférhetnek. De nem csak jó értelemben véve. Egy nem megfelelően kiépített és levédett rendszer körülbelül ahhoz hasonlítható, mintha a saját gépünkön sok platformot, vagyis felhasználói felületet alakítanánk

ki, és akadályoztatás nélkül tudunk az egyikből a másikba átjárni. Ez a legnagyobb veszélye a hálózati rendszereknek. Bármely pontján támadják is meg, a többi tag ugyanolyan veszélyben van, mint az az egy gép. Nyilvánvaló, hogy a fájlokat védeni kell, felhasználói jogokkal és jelszavakkal. Az internetes szerverek esetében alapvetően háromféle felhasználót különböztetünk meg:

A rendszergazda, vagy újabban superuser a gép irányítója. A microsoftos világban hívják még adminisztratornak, UNIX esetében root-nak, régebbi hálózatokon supervisornak, a WWW-ben webmasternek is. Ha valaki a superuser nevével lép be, és tudja a jelszót, akkor bármihez joga van, korlátlanul hozzáfér bármelyik fájlhoz, illetve a további jelszavakhoz. Élet és halál ura, vagyis usereket teremthet, korlátozhat, vagy ki is zárhat. A gépek feletti egyeduralmukat csak a gondatlanságuk, tudatlanságuk és hanyagságuk veszélyeztetheti.

A „user", más néven felhasználó, neki van neve és jelszava, joga viszont csak annyi, amennyit az előző személy engedélyez neki. Ha rendetlenkedik, nem tartja be a játékszabályokat, egy gombnyomással kizárják a csapatból és a gépből. Ő az átlagos felhasználó.

A „guest": vendég csak nevet kap (vagy még azt sem), jelszó nélkül. Annyi joga van, mint bármelyik vendégnek egy idegen helyen. Körbenézhet, kipróbálhat bizonyos dolgokat, programokat, de kizárólag csak azokat, amiket a házigazda engedélyez neki. Más hozzáférése nincsen. Ő egy átlagos böngésző a sok millió közül, aki szörfölget a világhálón.

A rendszer ellen támadókat tehát főleg a superuseri jogosultságok érdeklik, ennek megszerzése a végső céljuk. Erre több lehetőségük van. A „beépített" ember, a „tégla" a superuser által (is) használt számítógépbe valamilyen

trükkel bejuttat egy kis vírust. Ilyen például az egyik legismertebb, a NetBus. A NetBus egy úgynevezett trójai program. Ez annyit jelent, hogy a célgépre valahogy fel kell telepíteni a program szerver részét, melyhez aztán hozzá lehet kapcsolódni a klienssel. Akkor pedig nincs megállás.

A NetBus segítségével gyakorlatilag átvehető az irányítás az illető gépe felett, minden megtehető, ami neki jogában áll. A NetBus minden TCP/IP-kompatibilis hálózaton használható, beleértve az internetet is. Ami kell hozzá: Windows 95/98/NT 4. A NetBus egy gonosz krampusz! Ezek segítségével a támadó jogosan mondhatja, hogy „Jöttem, láttam, győztem!"

Egy másik fajta vírus semmi egyebet nem csinál, csak a felhasználók által elsőnek beírt karaktereket tárolja, a háttértár egy jól eldugott fájljában, például úgy, hogy figyeli a billentyűzetet. Emlékeznek még erre a Keyloggerinctelenség című fejezetből? Na most a superuser először nyilván a felhasználói nevét és a jelszavát írja be, a vírus tehát ezt is tárolja. A hacker az interneten keresztül leszedi a tárolt adatokat, innentől kezdve azt tesz, amit akar.

Sokkal veszélyesebb és profibb módszer az, mikor a fenti vírust bizonyos, nem publikált ftp (fájl-transzfer protokoll) parancsokkal maga a hacker juttatja be a feltörni kívánt szerverbe. Az ftp-ken, fájlcserélő programokon keresztül folyamatos támadásokra számíthatunk. A felületükön olyan programok vannak általában, amit sokan és szívesen használnak, ezért rendszeresen látogatják ezeket az „ingyen", vagy szűk körben elérhető fizetős helyeket anélkül, hogy tudnák, hogy ki és milyen szándékkal hozta létre azokat. Nem győzöm hangsúlyozni, hogy ne dőljenek be ezeknek a csapdáknak. Csak ellenőrzött helyről telepítsenek le és fel, vagy használjanak programokat!

A fent bemutatott módszerek a komoly védelmek, firewallok kijátszására szolgálnak. Kevésbé hatékony védelmet a kezdő hackerek is fel tudnak törni, kifejezetten e célra készült programok segítségével. Hackelő programok sajnos, szép számmal találhatóak a neten, a wannabek nagy örömére. A megszerzett passwordok birtokában bármilyen fájl fel- és letölthető, a honlap átszerkeszthető, sőt, kicserélhető.

Az „evil" (gonosz) persze nem áll meg az ilyen piti dolgoknál, ő például átirányít néhány milliócskát a saját bankszámlájára, esetleg nemzetbiztonsági adatokat szolgáltat ki az arra vevőknek. Ma már minden megtörténhet a bitek világában. Nincsen olyan terület, amely ne lenne veszélyeztetve. Aki az ellenkezőjét állítja, az nem is ért hozzá. A laikusoknak meg teljesen mindegy, őket úgyis csak az érdekli, hogy milyen idő lesz holnap.

Speciális esete a tudatos kalóztámadásnak az, amikor nem törik fel, hanem „mindössze" kivonják a forgalomból a célba vett szervert. Ennek két gyakori formája a DDoS és a robbanó levél. Mindkettő nagyon hatásos. A DDoS (Distributed Denial of Service) elsősorban az ftp-szervereket fenyegeti, de már készül a WWW-s változata is, ami még veszélyesebb lesz az általános felhasználókra.

A támadás úgy történik, hogy a hacker nagyszámú (több száz) kellőképpen meg nem védett szervernek elküld egy kis vírust (ilyen például a M-stream). Nyilvánvaló, hogy olyan szervereket keres meg erre a célra, amelyeken semmi különösebben fontos vagy védendő anyag nincs – nyüzsögnek az ilyenek a hálózaton, lehet, hogy az ön által használt szerver is éppen egy DDoS programot futtat...

A továbbiakban ezek mint rabszolgák, a kiadott parancsnak megfelelően, egy bizonyos pillanatban elkezdik egy-

szerre hívni a tönkreteendő célszervert, ami nem bírja a terhelést, ezért jó darabig elérhetetlen lesz azok számára, akik függnek tőle. Az üzleti életben, legfőképp az e-businessben pedig néhány nap elérhetetlenség teljes anyagi csőddel egyenlő, maga a biztos halál.

A robbanó levél is csak látszólag ártatlan: az e-mail csatolt fájljában elrejtett kis makrovírus csupán annyit tesz, hogy továbbküldi önmagát a levelezőprogram címjegyzékében szereplő összes címre. Igen ám, de az, aki az én címjegyzékemben szerepel, annak nyilván én is ott vagyok a címjegyzékében. Tehát rövidesen újra visszakapom a levelet, egyre több példányban – a vírus meg csak terjed és terjed, és a mail-szerver előbb-utóbb már csak ezeket a leveleket fogja továbbítani, rendes levelekre nem marad energiája.

Maga a konkrét folyamat elvileg megállíthatatlan, de azért védekezhetünk ellene, mégpedig úgy, hogy elfelejtjük az e-mail címünket és a címlistánkat, gyártunk egy újat, és még véletlenül sem lépünk be újra a régi postafiókunkba.

Ha szeretne mély benyomást tenni egy biztonsági szakértőre, mondja azt, hogy az elmúlt öt évben csak egyszer törtek be a rendszerébe. Ez is hihetetlenül hangzik egy szakember számára, de legalább nem fogja azt hinni, hogy még arra is képtelen, hogy észlelje a támadásokat. Amióta bármely számítógépet bármely másikkal összeköthetünk, a fő kérdés a számítógépes hálózatok biztonsága. A sok bizalmas információt megvédeni a külső támadásokkal szemben, mint például a vírusok, vagy a hackerek betörései, elég fontos feladat. Szükség van egy olyan mechanizmusra, amely megakadályozza a nem kívánt, „kártékony" adatok és programok beszivárgását rendszerünkbe.

Az interneten alapvetően kétfajta támadási forma létezik: a hálózatot alkotó gépek elleni, és a hálózati forgalom elleni akciók. Meg kell akadályoznunk, hogy bizalmas adataink illetéktelenek kezébe kerüljenek. A támadók nem válogatnak a módszerekben. A legelterjedtebb eszközeik a spyware, malware, backdoor alkalmazások, melyek a definíció alapján nem számítanak vírusnak, mégis temérdek problémát okozhatnak a célpontoknak.

Néhány alapvető és betartandó jó tanács a világhálót használóknak, ami mentőöv is lehet egyben:

- Minden e-mailt, amelyek nem személyes feladótól származnak, rögtön töröljön! Ezekhez tartoznak egyébként a kéretlenül beérkező e-mailek, amelyek egy ismert vállalattól (Microsoft, T-Online, Freenet) származnak, mert a spamküldők hamisíthatnak ilyen feladókat. Mivel általában az átlag felhasználók nincsenek közvetlen kapcsolatban ilyen nagy cégekkel, azok nem is fognak velük levelezni direktben, tehát a nevüket más használja fel, jogtalanul.
- A feladónak semmi esetre se válaszoljon, még ha ezt az e-mailben fel is kínálják! Spamküldők az ilyen üzenetekkel felügyelik, hogy megérkezett-e önhöz a postájuk. Soha ne kövessen linkeket az ilyen e-mailekből, akkor sem, ha kecsegtető az ajánlat, mert gyakran közvetlen, drága dialerekre mutató letöltési linkekről van szó, és a meggondolatlansága, kíváncsisága már a zsebére dolgozhat utána.
- A biztonsági beállításokat e-mail programjában állítsa olyan magasra, amennyire csak tudja! A pontos eljárásról érdeklődjön a gyártónál!
- Használjon több e-mail címet! Nyilvánosan látható internetes bejegyzésekhez, például vendégkönyvekben vagy newsgroupokban soha ne használja a személyes

e-mail címét! A spammerek használnak bizonyos „robot” programokat, amelyekkel az interneten e-mail címek után kutatnak, hogy azokat összegyűjtsék. Készítsen egy második, sőt harmadik e-mail címet, például a Yahoo-n vagy a Hotmail-en! A személyes e-mail címét csak megbízható embereknek (barátoknak, rokonoknak) adja tovább!

Az MS Windows a világ legelterjedtebb operációs rendszere – annak az összes előnyével és hátrányával. A hátrányokhoz tartozik mindenképpen, hogy szinte minden kártékony program, mint vírusok vagy trójai programok, de csaló-betárcsázó programok is a Windows és a hozzá tartozó Internet Explorer gyenge pontjainak támadására vannak kifejlesztve.

A megbízható és komoly szolgáltatók mindenről informálják ügyfeleiket, még arról is, ha szolgáltatásukat egy emelt díjas híváson keresztül lehet kifizetni. Más szolgáltatók nem világosítják fel a felhasználót a dialer (betárcsázó program) letöltésének körülményeiről és a keletkező költségekről. Hogy itt egy dialer letöltéséről van szó, amely a használat esetén jelentős többletköltséggel jár, elhallgatják! Nem véletlenül!

Ha mégis reklamálna valaki, a hó végi számláját elolvasva, csak széttárják a karjukat, és annyit mondanak, hogy „Sorry”, de senki nem tudja megállapítani, hogy valóban más használta a rendszeremet, így az én dolgom, hogy fizessek, vagy mehetek a bíróságra. Ez elég undorító eljárás, de sajnos ez van! A „Multimedia update” csupán egy a sok megnevezés közül, amikkel szolgáltatók a dialerjüket álcázzák. Nem árt az emlékezetünkbe vésni, mivel rendszeresen megjelennek a monitorjainkon ezek a feliratok.

CONCLUSIOrwell

Végkövetkeztetés

A Big Brother Művek virtuális gyárlátogatásának végére értünk. Feltárultak önök előtt olyan ajtók, amelyek mögé a hétköznapi életükben nincsen lehetőségük bejutni. Sajnos még mindig vannak olyan ajtók, melyekre a „TOP SECRET” (Szigorúan Titkos) felirat van írva, ezek egyelőre zárva maradtak számunkra.

Megismerhették a gyáróriás működtetőit és alkalmazottait, akik termékbemutatókat tartottak nekünk. Láthatták, hogy milyen szisztematikus és alapos munka folyik a gyár szigorúan védett objektumaiban, ahol rabszolgaként saját találmányaik és fejlesztéseik fogságában élik napjaikat a kiváló elméjű, de érzelmileg és szellemileg manipulált emberek. Gépek, robotok, komputerek kényszerítik őket arra, hogy Uraik parancsait maximálisan végrehajtsák.

Ebben a gyárban az összes „nagy elme” megfordult és megfordul ezután is, Leonardo da Vincitől kezdve, Einsteinen keresztül Bill Gates-ig. Ők azok, akik hozzáraktak(nak) az elődeik tudásához egy kicsit, és ezzel mozgásban tartják az „emberiség fejlődését”, a „Nagy MŰ” elkészülését, a „Totális Kontroll” kiépülését.

Mint láthatták, a Gyár területe egy labirintushoz hasonlít, és ha valaki nem ismeri ki magát benne, az könnyen elveszhet a sok információ között. Igyekeztem átfogó képet adni a jelen és a közeljövő várható eseményeiről.

Köszönetet mondok azoknak a szakembereknek, kollégáknak, akik saját szakterületeik specialistái, amiért megosztották velem a tudásukat, hogy aztán továbbadhassam

önöknek a számítástechnika, biztonságtechnika, biotechnika, haditechnika „vívmányairól" szóló híreket.

Saját bőrükön érezhetik, hogy az orwelli „élhető" világ megvalósult, sőt ebben élünk már, ami nem egyszerű feladat. Meddig tart ez az őrült száguldás? Hol van a vonat végállomása? Erre a kérdésre emberi elme nem tud választ adni. Mi, a felsőbbrendű élőlény földi képviselői naponta beikszelünk egy számot az élet naptárán, és azt mondjuk: megint eltelt egy nap az életünkből, ami azt jelenti, hogy földi pályafutásunk végéhez közelebb kerültünk.

A vonat viszont robog tovább. Van, aki önszántából ugrik ki belőle, mert rájön, hogy merre tart vele a vonat, van, akit kilöknek idő előtt, de a többség sebességmámorban úszva, eufórikus állapotban halad előre, megállás nélkül a sínpár végén álló ütközőig, melyre az van felírva, hogy:

THE END...

ádiófrekvenciás chipkártyák*

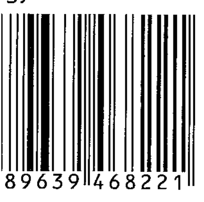
íszazonosítással működő bankjegykiadó automaták

*emzetbiztonsági érdekből a magándokumentumokon
hatatlan azonosítási kódot rögzítő printerek*

*személyiség átprogramozását lehetővé tevő, bőr alá
ültetett nanotechnológiás mikrochipek.*

legújabb csúcstechnika, amit ma még föld alatti tit-
laboratóriumokban tesztelnek, holnap megérke-
t az otthonokba, a közterekre, és ott lapulhat szinte
ndenki zsebében.
totális kontroll felé vezető úton már nincsenek cél-
mélyek: minden és mindenki a megfigyelés tárgyává
hat.
elyek a legérzékenyebb veszélyforrások, és hogyan
lekezhetünk a kiszolgáltatottsággal szemben? Kinek
at érdekében, hogy az embereket kitörölhetetlenül
át vagy ellenség címkével lássa el?
eves biztonságtechnikai szakértő, Dave Forrest szá-
s eddig nem publikált információt és fordulatos tör-
etet feldolgozó könyve ezekre a kérdésekre keresi a
aszt.

gy. ár: 2499 Ft



89639 468221

ww.sprinterkiado.hu

FOCUS

DAVE FORREST BARÁT VAGY ELLENSÉG?

FOCUS

BARÁT VAGY ELLENSÉG?

A TOTÁLI
KONTROL
FORGATÓKÖNYV